REPORTING DATA BREACHES: IS FEDERAL LEGISLATION NEEDED TO PROTECT CONSUMERS?

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JULY 18, 2013

Serial No. 113–71

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
86–395 WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

RALPH M. HALL, Texas
JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

LEE TERRY, Nebraska
Chairman

LEONARD LANCE, New Jersey
Vice Chairman
MARSHA BLACKBURN, Tennessee
GREGG HARPER, Mississippi
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVE B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
JOE BARTON, Texas
FRED UPTON, Michigan, *ex officio*

JANICE D. SCHAKOWSKY, Illinois
Ranking Member
G.K. BUTTERFIELD, North Carolina
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
JOHN D. DINGELL, Michigan
BOBBY L. RUSH, Illinois
JIM MATHESON, Utah
JOHN BARROW, Georgia
DONNA M. CHRISTENSEN, Virgin Islands
HENRY A. WAXMAN, California, *ex officio*

CONTENTS

REPORTING DATA BREACHES: IS FEDERAL LEGISLATION NEEDED TO PROTECT CONSUMERS?

THURSDAY, JULY 18, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 11:04 a.m., in room 2123 of the Rayburn House Office Building, Hon. Lee Terry (chairman of the subcommittee) presiding.

Present: Representatives Terry, Lance, Harper, Guthrie, Olson, Kinzinger, Bilirakis, Johnson, Long, Barton, Schakowsky, Sarbanes, McNerney, Barrow, Christensen, and Waxman (ex officio).

Staff present: Kirby Howard, Legislative Clerk; Nick Magallanes, Policy Coordinator, Commerce, Manufacturing, and Trade; Brian McCullough, Senior Professional Staff Member, Commerce, Manufacturing, and Trade; Gib Mullan, Chief Counsel, Commerce, Manufacturing, and Trade; Andrew Powaleny, Deputy Press Secretary; Shannon Weinberg Taylor, Counsel, Commerce, Manufacturing, and Trade; Michelle Ash, Democratic Chief Counsel; and Will Wallace, Democratic Professional Staff Member.

OPENING STATEMENT OF HON. LEE TERRY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEBRASKA

Mr. TERRY. Good morning. I recognize myself for an opening statement.

In today's economy, nearly everyone leaves a digital footprint. Even if you made a concerted effort to avoid smartphones, laptops, and social media, although I have not found that person, you would have a difficult time keeping your personal information from being held in an electronic database somewhere.

Consumers should have the peace of mind that their data is protected in a responsible way. But with all types of nefarious activities online, cyber criminals are finding new ways and, frankly, seem to be very consistent in their wishes to steal data. So in the event that our personal data becomes exposed, we need to be able to trust that the companies in possession of that data will notify us of the exposure. And certainly it is in those companies' best interest to notify promptly and clearly in order to preserve a trusting relationship with their customers.

Given these considerations, the question before us is: What are the rules of the road for companies that experience a breach in their data stores? Currently, the laws that govern data breach notification are a patchwork of state- and territory-specific statutes. Unfortunately, they tend to differ from each other in many ways. For example, while a number of States have adopted a common definition of personal information, even more States have adopted alterations to that definition, and those vary unpredictably. The definition is important because it triggers the duty to notify of a breach. Three States include encrypted or redacted data in the definition of personal information, whereas the rest do not. Five States include public records in the definition. Meanwhile, four States protect an individual's date of birth and mother's maiden name as personal information.

With at least 48 of these various state- and territory-specific laws on the books, you can see how the cost of compliance could add up. The global price tag of cyber crime has been calculated at around $110 billion annually, and we should not add unnecessary compliance costs to this. Adding to the confusion, these laws also tend to vary on the number of days that can elapse after a breach before notification as well as the method of notification.

Even small breaches can cause a compliance headache. In one recent example, a large company experienced a breach where the personal information of just over 500 consumers was compromised. In comparison to other breaches involving tens of millions of consumers, this may seem small. Yet it turns out that these 500 consumers lived in 44 different States and therefore had to be notified pursuant to 44 different sets of rules.

We must remember that where a breach in data is an intentional intrusion from the outside, for example, if it is done by a hacktivist, a foreign agent or a run-of-the-mill criminal, the company holding the data is also a victim. Burdening these entities with overly complicated notification rules is not a solution to the harms that result from the exposure of that personal information held by the company.

And with that, I look forward to hearing the testimony of our witnesses and learning about whether or not we can improve the current legal landscape for breach notification.

[The prepared statement of Mr. Terry follows:]

PREPARED STATEMENT OF HON. LEE TERRY

- In today's economy nearly everyone leaves a digital footprint.
- Even if you made a concerted effort to avoid smart phones, laptops, and social media, you would have a difficult time keeping your personal information from being held in an electronic database somewhere.
- Consumers should have the peace of mind that their data is protected in a responsible way.
- But, with all types of nefarious activities online, cyber criminals are finding new ways to steal data.
- So in the event that our personal data becomes exposed, we need to be able to trust that the companies in possession of our data will notify us of the exposure.
- And certainly it is in those companies' best interest to notify promptly and clearly in order to preserve a trusting relationship with consumers.
- Given these considerations, the question before us is: What are the rules of the road for companies that experience a breach in their data stores?
- Currently, the laws that govern data breach notification are a patchwork of state- and territory-specific statutes.

• Unfortunately, they tend to differ from each other in many ways.
• For example, while a number of states have adopted a common definition of "personal information," even more states have adopted alterations to that definition, and those vary unpredictably.
• This definition is important because it triggers the duty to notify of a breach.
• Three states include encrypted or redacted data in the definition of "personal information," whereas the rest do not.
• Five states include public records in the definition. Meanwhile, four states protect an individual's date of birth and mother's maiden name as "personal information."
• With at least 48 of these various state- and territory-specific laws on the books, you can see how the cost of compliance could add up.
• The global price tag of cyber crime has been calculated at around $110 billion annually, and we should not add unnecessary compliance costs to this.
• Adding to the confusion, these laws also tend to vary on the number of days that can elapse after a breach before notification as well as the method of notification.
• Even small breaches can cause a compliance headache: In one recent example, a large company experienced a breach where the personal information of just over 500 consumers was compromised.
• In comparison to other recent breaches involving tens of millions of consumers, this may seem small. Yet it turns out that these 500 consumers lived in 44 different states and therefore had to be notified pursuant to 44 different sets of rules.
• We must remember that where a breach in data is an intentional intrusion from the outside-for example, if it is done by a "hacktivist", a foreign agent, or a run-of-the-mill criminal-the company holding the data is also a victim.
• Burdening these entities with overly complicated notification rules is not a solution to the harms that result from the exposure of personal information.
• And with that, I look forward to hearing the testimonies of our witnesses and to learning about whether we can improve the current legal landscape for breach notification.

Mr. TERRY. At this point, I will yield back my time and recognize the ranking member, Jan Schakowsky, for her statement.

OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

Apropos of this hearing, it has just been reported this very morning that Anonymous claims to have hacked into 1,800 email accounts of Members of Congress and their staffs. So that is apparently in the news. I don't know to what extent that has been confirmed. So I look forward to hearing from our witnesses about this issue and steps that can and should be taken to address it.

As a long-time consumer advocate, I believe that the public does have a right to be informed if their personal information such as names, email addresses, passwords, home addresses, health and financial data is compromised. As more and more information moves online, it is equally important to ensure that precautions are taken to keep that data secure.

Less than 2 years ago following the breaches of data at Citicorp, Epsilon and Sony, a report of the data security from Protegrity found that personal information was "highly valuable" to cyber criminals but "vastly unprotected." Since then, it seems to me, and you will set me straight, little has changed. Last year, 680 confirmed data breaches compromised almost 28 million records. Many of those could have been prevented with relative ease had the entities holding the data followed known best practices. This is clearly a major issue which the private sector has not done enough on its own to address, and one of great concern, I believe, to the public.

Almost every state and territory including my home State of Illinois has adopted data breach standards. While national standards might be needed to adequately address this issue, I want to make clear, my view is that any federal law should not weaken strong State laws. In addition, any federal response should establish a baseline so that every American can be assured some level of data protection, not just notification after the fact.

This subcommittee has several questions to answer as we consider data breaches and hopefully data security as well. What specific measures should be taken to protect personal information stored online? When should consumers be notified of a breach? What role should the federal government play in ensuring that those steps are taken? I believe that entities that store important data should act proactively to defend that information and the consumer should be notified if a breach could result in personal harm.

The DATA Act, introduced by Mr. Rush and passed by voice vote just 4 years ago, would have taken those steps to protect American consumers. I was a cosponsor of that bill along with Mr. Barton, and I believe it should be the framework for bipartisan legislation in this Congress.

Again, I look forward to hearing from our witnesses today about what can and should be done to address breach notification and data security. I hope that this subcommittee can work constructively toward a bipartisan solution to this major issue that impacts all of us.

Thank you. I yield back.

Mr. TERRY. And that is our goal.

At this time the chair recognizes the chairman emeritus, Mr. Barton.

OPENING STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BARTON. Thank you, Mr. Chairman, and I am very happy that you are having this hearing. As Congresswoman Schakowsky just pointed out, this is an issue that is not unfamiliar to the subcommittee or the full committee. Going back to my tenure as chairman in 2005 and 2006, we passed a bill out of committee but it didn't go to the floor. Under Mr. Dingell's chairmanship and Mr. Waxman's chairmanship, again, we passed bills that came out of committee and we have even had one bill that passed the floor of the House but it wasn't taken up in the Senate. The last Congress, we passed a bill out of this subcommittee but it was not taken up at full committee.

So this is an issue that we all have general agreement on. As Congresswoman Schakowsky has pointed out, it is not a partisan issue. Hopefully under your leadership, Mr. Chairman, and Mr. Upton's leadership at the full committee, we will pass something in this committee, on the floor and get the other body to take it up.

This year alone, our last year, in 2012, there were 470 breaches that meet the definition, and so far this year, there have been 326 breaches. This is an issue that is not going to go away. It would appear to be obvious that we need a federal bill instead of a patchwork of State bills, and I would agree with what Congresswoman

Schakowsky said, that a federal bill should be a baseline bill and not a bill that limits the States.

With that, Mr. Chairman, again, thank you for your leadership. I believe you are the man who can make this happen, subcommittee, full committee, the floor and then with the other body. And with that, I will yield back.

Mr. TERRY. No pressure there.

Are there any other Republicans on this side that wish to have time yielded?

Mr. BARTON. If not, Mr. Chairman, I yield back.

Mr. TERRY. Then we will yield back.

Before I announce our panel and start our testimony, an announcement of sorts—oh, Henry is here, so while he is sitting down, my announcement is, we will recess at noon and reconvene if it is still necessary to. I have a feeling that there is going to be enough questions that we will reconvene at 1 o'clock but break at noon, and I recognize the full committee ranking member, the gentleman from California is recognized for 5 minutes.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you very much, Mr. Chairman. I welcome all of our witnesses today.

Our subcommittee is going to address the federal role in data breach notification. It is alarming just how common data breaches have become. Since 2005, at least 600 million records containing consumers' personal information have been compromised as a result of more than 3,800 data breaches in the United States. At least 72 million personal records have been compromised only in the time since July 2011, when the Subcommittee last considered this issue.

Every type of entity has proven vulnerable, including private sector companies of all sizes, colleges and universities, and federal, State, and local governments. Breaches result from a wide variety of causes. External criminal attacks, dishonest insiders, and simple negligence can all be responsible for compromising consumers' personal information. Moreover, in recent months, it has become abundantly clear that commercial data breaches can also result from State-affiliated cyber attacks.

Consumers face severe threats to their financial well-being when data like banking information or Social Security numbers are compromised. In 2012 alone, more than 12 million U.S. adults were victims of identity theft or similarly costly forms of fraud. Less reported, but also of concern, is when breaches, non-financial in nature, threaten consumers' privacy, including breaches involving health-related information, biometric data, or a person's precise location.

Nearly all U.S. States and territories now have laws that require notice for their own residents when a data breach occurs. These laws vary greatly, but several of these laws are quite strong, ensuring that consumers receive prompt, clear and complete notification when their personal information is breached and providing them with resources to protect their financial well-being. I am glad that

these laws have been enacted, but after-the-fact breach notification is only half of what is needed. The private sector also must take reasonable steps to safeguard personal information.

When it comes to information security, prevention is the best medicine. Research shows that the vast majority of attacks on commercial data—78 percent according to the Verizon RISK Team—utilize simple tactics easily thwarted by basic security infrastructure and procedures.

There are many companies that take information security very seriously and work diligently to combat this problem, and perhaps there will always be cyber crime. But unfortunately, there are also companies that are not doing enough to prevent breaches, and consumers are paying the price.

As the subcommittee moves forward with its work on information security, I strongly encourage all members to keep two points in mind. First, federal legislation must not move backward by undermining those States with strong breach notification laws. And second, effective security for consumers' personal information indisputably requires both breach notification and reasonable safeguards for commercial data.

I look forward to the testimony we are going to get today and our discussion of this issues today and in the future and I hope we can work together to deal with this important issue.

Mr. TERRY. I appreciate that, Mr. Chairman.

At this time I am going to introduce our full panel, and then we will start with Mr. Richards. Mr. Richards is the Senior Vice President of Federal Government Affairs for TechAmerica. We have Dan Liutikas, Chief Legal Officer, CompTIA. We have Mr. Jeff Greene, Senior Policy Counsel, Cybersecurity and Identity, Symantec Corporation. We then have Debbie Matties, CTIA—The Wireless Association Vice President of Privacy. We have Andrea Matwyshyn, Assistant Professor of Legal Studies and Business Ethics at the Wharton School, University of Pennsylvania. David Thaw will complete our testimony, and he is Visiting Assistant Professor of Law at the University of Connecticut School of Law.

You will see little lights down there. Green means go. At 4 minutes, the yellow line will come on and that should be a sign, if you got a full page or two left, you may want to skip to the conclusion. The red light means I'm going to lightly tap the gavel, and so I appreciate keeping it to the 5-minute mark, especially since we have been kind of put on an awkward, tight schedule today.

So Mr. Richards, you may begin. You are recognized for your 5 minutes.

STATEMENTS OF KEVIN RICHARDS, SENIOR VICE PRESIDENT, FEDERAL GOVERNMENT AFFAIRS, TECHAMERICA; DAN LIUTIKAS, CHIEF LEGAL OFFICER, COMPTIA; JEFFREY GREENE, SENIOR POLICY COUNSEL, CYBERSECURITY AND IDENTITY, SYMANTEC CORPORATION; DEBBIE MATTIES, VICE PRESIDENT OF PRIVACY, CTIA—THE WIRELESS ASSOCIATION; ANDREA M. MATWYSHYN, ASSISTANT PROFESSOR OF LEGAL STUDIES AND BUSINESS ETHICS, THE WHARTON SCHOOL, UNIVERSITY OF PENNSYLVANIA; AND DAVID THAW, VISITING ASSISTANT PROFESSOR OF LAW, UNIVERSITY OF CONNECTICUT SCHOOL OF LAW

STATEMENT OF KEVIN RICHARDS

Mr. RICHARDS. Thank you. Mr. Chairman, Ranking Member Schakowsky, and distinguished members of the subcommittee, thank you for the opportunity to testify today and for convening this hearing on the important issue of data breach notification. I am Kevin Richards, Senior Vice President of Federal Government Affairs of TechAmerica, a leading technology association representing the world's premiere technology companies from the information and technology communications sector at the state, federal, and international level.

The topic of today's hearing is an issue of great concern to our members who view the unauthorized disclosure and use of personal information as a threat that erodes public confidence in a connected world. TechAmerica's member companies understand better than anyone the nature of cyber threats that America faces today and what must be done in order to protect consumers' information from data breaches.

The rapid growth of the collection of information in electronic form has provided consumers, businesses and governments with tremendous opportunities from revolutionizing the way medical care is provided to enhancing government services, to enabling a free Internet with more opportunities appearing daily. However, this collection of data has also resulted in a concomitant exposure of companies to risks and liabilities arising from the collection, use, storage and transmission of information, particularly sensitive information about individuals.

TechAmerica strongly believes that if a breach occurs that poses a significant risk of serious harm, that there should be a consistent national policy to ensure that customers and consumers are notified in an appropriate manner.

Today, 48 different State jurisdictions in the United States have data breach notification laws, and while many businesses have managed to adapt to these various laws, a properly defined data breach notification standard would go a long way to guide organizations on how to address cyber threats in their risk management policies. It also would help prevent breaches and give guidance on how best to respond if an organization should fall victim to a reach caused by an attack. It would be particularly helpful for smaller businesses, many of whom cannot afford teams of lawyers to navigate 48 breach standards should something bad actually happen.

National data breach legislation should be carefully crafted and in particular be technology-neutral to help organizations prevent

and respond to security incidents while avoiding costly, burdensome rules that would not provide any real protection to consumers and free security innovation. Such legislation will provide much-needed regulatory relief to companies facing conflicting legal obligations under today's patchwork of State laws.

TechAmerica has been a leader in calling for a strong, preemptive, and uniform national breach notification law. Federal legislation that promotes notification to consumers when their data has been compromised is needed, and can effectively help restore consumers' online trust and confidence.

The first objective of federal data breach notification legislation should be to establish a uniform national standard and preempts the current patchwork of existing State laws while providing a safe harbor for those entities that take steps to protect their systems from breaches and render data unreadable, undecipherable and unusable in order to protect individuals from harm. The following recommendations are a result of lessons learned from the implementation of regimes by the current 48 different State jurisdictions in the United States and which serve as a good benchmark for drafting potential legislation.

One, legislation must establish a single, uniform preemptive standard. Two, a meaningful threshold for notification should be established. Three, define carefully the kind of personally identifiable information that is covered by notification requirements. Four, avoid mandating specific technologies while encouraging the adoption of good practices. Five, when third-party managed data notification is required, avoid consumer confusion. Six, a federal law should do more than the patchwork of state laws to protect consumers.

In conclusion, TechAmerica believes that the patchwork quilt of state laws and existing requirements needs to be overhauled by a uniform preemptive national standard based on the risk of harm. This would be in addition to the significant protection consumers receive today. With the chairman's permission, TechAmerica would like to request the submission of TechAmerica's national data breach legislative principles for inclusion in the record for today's hearing.

Mr. TERRY. Unanimous consent to allow? Hearing no objection, so allowed.

Mr. RICHARDS. Thank you. We are happy to offer assistance to the committee and work with you as the legislative process moves forward.

Thank you for allowing me the privilege to appear today in order to share TechAmerica's views on the important of data breach notification. I would be happy to answer any questions that the committee may have at this time.

[The prepared statement of Mr. Richards follows:]

TechAmerica

Prepared Testimony and
Statement for the Record of

Kevin M. Richards
Senior Vice President
Federal Government Affairs
TechAmerica

Before the

U.S. House Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing and Trade

Hearing on

"Reporting Data Breaches:
Is Federal Legislation Needed to Protect Consumers?"

Thursday, July 18, 2013
2123 Rayburn House Office Building

INTRODUCTION

Mr. Chairman, Ranking Member Schakowsky and distinguished members of the subcommittee, thank you for convening this hearing and for bringing focus on the current state of consumer data breach notification in today's digital age. TechAmerica appreciates the opportunity to provide our insights as the Subcommittee on Commerce Manufacturing and Trade explores the effectiveness of current state data breach laws, and considers whether Congress should enact a national breach notification standard.

My name is Kevin Richards. I am the Senior Vice President for Federal Government Affairs of TechAmerica, an association representing the world's leading premiere technology companies of all sizes. TechAmerica[1] is the leading voice for the U.S. technology industry - the driving force behind productivity growth and job creation in the United States and the foundation of the global innovation economy.

We commend the subcommittee for making data breach notification a priority. This issue is a matter of great concern for our member companies that engage in global electronic commerce and provide much of the infrastructure to make e-commerce possible. Unauthorized disclosure and use of personal information erodes public confidence in the online world, and consumer notification when a breach has occurred gives consumers the knowledge and tools to protect them from possible harm.

TechAmerica and its member companies strongly support requiring entities that disclose sensitive personal information about consumers to notify consumers in appropriate circumstances, notably when there is a significant risk of harm. The question the committee is addressing today, whether federal legislation is necessary to protect consumers, is the right question to ask. State laws often vary needlessly and in some cases don't make sense. Therefore, we do believe that federal legislation is, in fact,

[1] TechAmerica is the leading voice for the U.S. technology industry – the driving force behind productivity growth and job creation in the United States and the foundation of the global innovation economy. Representing premiere technology companies of all sizes, we are the industry's only trade association dedicated to advocating for the ICT sector before decision makers at the state, federal and international levels of government. With offices in Washington, D.C., Silicon Valley, Brussels and Beijing, as well as regional offices around the U.S., we deliver our members top tier business intelligence and networking opportunities on a global scale. We are committed to expanding market opportunities and driving the competitiveness of the U.S. technology industry around the world.

necessary. However, some technology companies are not experiencing difficulties in complying with the various state data breach notification laws and for these firms a law that codifies one federal set of regulations and pre-empts state laws would be helpful, but not vital. Therefore, we believe that it is important that if Congress is going to address this issue, legislation needs to be done correctly and strike the right balance.

DATA BREACHES: ASSOCIATED BUSINESS RISKS

The rapid growth of the collection of information in electronic form has provided consumers, businesses and governments with tremendous opportunities, from revolutionizing the way medical care is provided, to enhancing government services to enabling a free internet, with more opportunities appearing daily. As Congress explores possible legislative responses to this issue, it is important to avoid any unintended consequences that legislation could have in this sensitive area.

However, this collection of data has also resulted in a concomitant exposure of companies to risks and liabilities arising from the collection, use, storage and transmission of information, particularly sensitive information about individuals.

There is a growing body of law directed at protecting personal information in the U.S. at both the state and federal levels, and in other countries, and notifying and empowering consumers with information about data breaches and the steps they can and should take to protect themselves in the event of a data breach. Many of these laws focus on the types of personal information that is often the subject of data breaches. This has likely mitigated the potential harm to consumers that may occur as a result of a data breach.

TechAmerica has been a leader in calling for a coherent, pre-emptive and meaningful national breach notification law. It is our desire in this hearing to share our experience with existing "breach notification" regimes, with the goal of providing "lessons learned" that will assist the committee in its examination of this important issue.

In the simplest terms, breach notification is one tool to respond to breaches when they occur. Breach notification requirements should also be focused on providing consumers appropriate notice about potential harm.

Any federal framework should provide for breach notification when there is, in fact, only a significant risk that identity theft has or is likely to occur. Without establishing a meaningful threshold and relevant requirements for notification, there is a very real likelihood of unintended, negative consequences for consumers, business entities and public authorities.

LESSONS LEARNED: TECHAMERICA'S POSITION ON A FEDERAL DATA BREACH LAW

TechAmerica believes that breach notifications should be required in those instances where there is a substantial risk of harm to a consumer. Federal legislation that promotes notification to consumers when their data has been compromised is needed and can effectively help restore consumers' online trust and confidence.

The first objective of federal data breach notification legislation should be to establish a uniform national standard and provide pre-emption of state laws. If a company does business in different states, they will usually notify in every state, even if their customers were not affected there and even if the state in question does not have an explicit breach notification requirement.

We urge the subcommittee to consider legislation which would provide a national data breach notification standard that creates a national standard and pre-empts the patchwork of existing state laws, while providing for safe harbor for those entities that take steps to protect their systems from breaches and render data unreadable, undecipherable, and unusable in order to protect individuals from harm.

The issue of data breach notification and when it should be provided to consumers first burst on to the scene in 2005, when ChoicePoint announced that it had compromised the records of 163,000 people and paid a record fine to the Federal Trade Commission (FTC). Since then, while Congress, the FTC and other federal

agencies have addressed various concerns about data breach notifications in fits and starts, the states and the market have taken the lead in addressing this problem.

Today, there are forty-eight different state jurisdictions in the United States[2] that have implemented data breach notification laws, and the U.S. Federal Trade Commission (FTC) is bringing actions under its existing authority[3] for failure to maintain or disclose security practices. The following recommendations are a result of the lessons learned from the implementation of these regimes and serve as a good benchmark for the drafting of potential federal legislation to ensure appropriate consumer protections:

1) **Legislation must establish a single, uniform, preemptive standard.** Any federal standard must be uniform and pre-emptive. Adding a fifty-first standard and/or layering on additional federal requirements on top of current state requirements would only add confusion, cost and risk to the system. The current patchwork quilt of current state data breach notification laws is a burdensome compliance challenge which is confusing for both businesses and consumers. One strong, uniform federal system that promotes predictability and certainty for consumers, consumer protection authorities and businesses, and reduces duplication, compliance costs and inconsistencies, is much preferable.

2) **Establish a meaningful threshold for notification.** To ensure that notification is part of a coherent approach to combating the pernicious effects of identity theft, a legal regime should require notification to consumers when the security of sensitive personal information has been breached in a manner that creates a significant risk of identity theft. The establishment of a meaningful threshold is essential as there may be direct and harmful unintended consequences that may be associated with broad notification. For example, the experiences with notification regimes to date have demonstrated that consumers have been subjected to fraud scams

[2] A generally reliable, publicly available resource that summarizes the state data breach laws has been prepared by the Perkins Coie (Law Firm), "Security Breach Notification Chart":[Link: http://www.perkinscoie.com/files/upload/PS_12_04SecurityBreachNotificationLawChart.pdf].

[3] E.g., primarily Section 5 of the FTC Act for deceptive and unfair trade practices. See, also, Children's Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA).

and "phishing" attacks when bad actors hear through the media about notifications, and a meaningful threshold predicated on a "significant risk" standard is essential to avoid over-notification of consumers, and minimizes the risk of fraud and identity theft that could result from consumer confusion. As former FTC Chairman Deborah Majoris has suggested, over-notification will cause "consumers [to] become numb if they are continuously notified of every breach."

3) **Define carefully the kind of personally identifiable information that is covered by notification requirements.** Central to an effective framework is a meaningful definition of "sensitive personal information" that is relevant to combating the pernicious effects of identity theft. It is essential that a careful circumscribed set of "sensitive personal information" be the basis for determining whether any notification should occur. It should not include elements that are widely used in commerce to facilitate transactions. It also makes no sense to require companies to impose additional security requirements on or notify consumers of security breaches on information that is already widely available and in the public domain.

4) **Avoid mandating specific technologies, while encouraging the adoption of good practices.** As part of the inquiry into whether "sensitive personal information" has been released in a way that may be harmful to consumers, TechAmerica urges the Committee to take into account whether the information that may have been accessed or released is usable. For example, a number of security methods and practices are available to businesses and government, including encryption, truncation, access controls, anonymization and redaction that would render any data that is breached unusable. In those instances, the requirement to notify consumers is unnecessary. To single out one method to secure data in legislation, such as encryption, suggests, if not outright mandates a de facto exclusive means to avoid notification, and creates a false sense of security. Singling out one methodology would not be in the overall best interests of the security marketplace, since it may reduce the development and use of diverse and innovative security tools.

5) **Where third parties manage data, and notification is required, avoid consumer confusion.** In cases where a 3rd party manages "sensitive personal information" of consumers for entities that own or possess sensitive personal information, notification requirements should be constructed to avoid consumer confusion. The best way to achieve this end is to obligate the third party to notify the entity that owns or licenses the data – i.e., the entity that has the relationship with the person whose sensitive personal information may have been breached. The entity that owns or licenses the sensitive personal information should, in turn, notify the end user or consumer. Otherwise, individuals are unlikely to recognize the source of the notice and thus unlikely to act in a manner to protect them, which is the object of notification regimes.

6) **A federal law should do more than the patchwork of state laws to protect consumers.** While TechAmerica believes that a uniform, national standard that protects consumers is more desirable than the current patchwork, Congress needs to be careful to ensure that any federal law that is enacted is careful to build on the experience of the states, not undermine the significant protections that consumers currently have at the state level.

CONCLUSION

In conclusion, TechAmerica believes that the "patchwork quilt" of state laws and existing requirements needs to be overhauled by a uniform, pre-emptive standard based on the risk of harm. This would be an effective addition to the significant protection that consumers receive today. Please find attached a copy of TechAmerica's National Data Breach Legislative Principles which we'd like to submit to the Record for today's hearing proceedings.

Mr. Chairman and members of the subcommittee, TechAmerica greatly appreciates the opportunity to testify today. We share the goal of the House Energy and Commerce Committee to help protect consumers and mitigate the potential harm posed by data breaches. We are happy to work with you as the legislative process moves forward.

Thank you for allowing me the privilege to appear here today in order to share TechAmerica's views on the important issue of data breach notification. I'd be happy to answer any questions that the committee may have at this time.

Mr. TERRY. Thank you very much.
And now, Mr. Liutikas, you have your 5 minutes.

STATEMENT OF DAN LIUTIKAS

Mr. LIUTIKAS. Good morning, Chairman Terry, Ranking Member Schakowsky, and distinguished members of the House Subcommittee on Commerce, Manufacturing, and Trade. This testimony is submitted on behalf of the 2,000 members of the Computing Technology Industry Association, also known as CompTIA, a not-for-profit trade association.

CompTIA is also the leading developer and provider of vendor-neutral education, IT workforce certifications including A+, Security+ and Network+, and organizational credentials such as the Security Trust Mark.

My name is Dan Liutikas, and I am the Chief Legal Officer of CompTIA. Prior to CompTIA, I was an attorney in private practice focusing on corporate technology and intellectual property matters, primarily for the small- to medium-size business. I am a native of Chicago, Illinois, and was born to immigrant parents from Lithuania. My father opened his own television repair shop and then later started a construction business. My mother started her own restaurants, delis, and banquet halls. Both lived the American dream by being entrepreneurial and starting their own small businesses. From my own experience, I submit that small business owners don't want handouts.

Like the businesses started by my parents, many of our members are small- to medium-sized businesses expect that they are IT solution providers that help other small- to medium-sized businesses set up IT systems and manage data. They also just want a fair shot at pursuing the American dream. In the context of today's hearing, that means eliminating unnecessary barriers to entry such as redundant and burdensome regulations. With that context, let me state upfront that our membership supports a federal approach to data breach notification.

It is hard to believe that it has been 10 years since California became the first State in the country to enact a State data breach notification law. Today, there are 46 states, D.C., and several territories that enacted data breach notification laws. Data breach notification standards are clearly a relevant concern for millions of users sharing information through the Internet and for information being stored in various forms.

A federal approach will bring clarity and certainty not only to small businesses but also to consumers who may not be aware of the notice obligations of a particular State's data breach notification law or even when such obligations may apply.

We appreciate the opportunity to submit our written testimony that provides greater details on the burdens of the current patchwork of State laws and the way in which advancements in mobile technology exacerbate those burdens. Therefore, I would like to spend the balance of my time on a solution.

Based on our collective experience and outreach efforts, we believe that the IT industry will be receptive to a national data breach reform framework that contains the following six principles.

Number one, there should be a single national federal standard for data breach policy. Businesses which conduct commerce over multiple States need the certainty and efficiency that a national standard would provide.

Number two, Congress and the FTC should not mandate specific technology or methods for data security practices. The environment for data security is constantly evolving, so any regulation should focus on promoting validated industry standards for security, rather than a single quickly outdated solution.

Number three: There should be an exemption from notification requirement for entities that deploy technology or methods such as encryption and other technologies that render data unusable or unreadable by hackers as a harm-prevention measure.

Number four, all enforcement and penalties for data breach law should be administrated by a central government agent instead of State Attorneys General, except in cases where the federal agent can or has not acted.

Number five, entities compliant with existing data breach legislation such as the Gramm-Leach-Bliley Act should be exempt from new regulation. We should not reinvent the wheel or create conflicting of overlapping regulations.

And number six, notification should occur on a reasonable time frame, which includes allowances for risk assessment and any necessary law enforcement procedures or investigation. Notification should be focused on events where there is a possibility of actual harm including a minimum threshold of affected individuals.

In closing, I want to reiterate that we believe that a national data breach framework is in the best interest of both consumers and small- to medium-sized businesses.

Thank you again for the opportunity to share our perspective on the issue of data breach notification reform, and I look forward to our discussion on how to best approach this issue, and I would be happy to answer any questions.

[The prepared statement of Mr. Liutikas follows:]

Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers

House Subcommittee on Commerce, Manufacturing and Trade

July 18, 2013

Submitted by:

Dan Liutikas, Chief Legal Officer

On Behalf of

The Computing Technology Industry Association (CompTIA)
515 2nd Street, NE, Washington, DC 2002

Computing Technology Industry Association (CompTIA)
Public Advocacy
515 2nd St NE
Washington, DC 20002
202-503-3624

Introduction

Good afternoon, Chairman Terry, Ranking Member Schakowsky and distinguished members of the House Subcommittee on Commerce, Manufacturing, and Trade. This testimony is submitted on behalf of the Computing Technology Industry Association (CompTIA).

My name is Dan Liutikas and I am the Chief Legal Officer of CompTIA. Prior to CompTIA, I was an attorney in private practice focusing on corporate, technology and intellectual property matters.

I am a native of Chicago, Illinois and was born to immigrant parents from Lithuania. My father learned how to fix televisions for a national retailer until eventually opening his own television repair shop and then later starting a construction business. My mother waited tables at restaurants and then started her own restaurants, delis and banquet halls. Both lived the American dream by being entrepreneurial and starting their own small businesses. From my own experience I submit that small business owners don't want handouts. They just want a fair shot at pursuing the American dream. In the context of today's hearing, that means eliminating unnecessary barriers to entry, such as redundant and burdensome regulations.

I am here today on behalf of the 2000 members of the Computing Technology Industry Association, many of whom are small business owners as well. CompTIA is a non-profit IT trade association. Our members are at the forefront of innovation and provide a critical backbone that supports broader commerce and job creation. Our membership includes computer hardware manufacturers, software developers, technology distributors, and IT specialists that help organizations integrate and use technology products and services. CompTIA is also the leading developer and provider of vendor-neutral IT workforce certifications, including A+, Security+ and Network+.

The Need for Data Breach Notification Reform

It is hard to believe that it has been 10 years since California became the first state in the country to enact a state data breach notification law. To provide some perspective, 10 years ago the majority of people accessed their digital data from desktop computers, and the mobile device industry was in its infancy. In 2002, Nokia introduced the world's first camera cell phone, and in 2003, Samsung developed the first cell phone with multiple screens. Back then the innovation was a screen on the outside of the phone to allow users to view incoming calls without having to open up their phones.[1]. Within a couple of years there will be more mobile devices than people and more people will access the

[1] http://www.hongkiat.com/blog/evolution-of-mobile-phones/.

Internet via a mobile device than desktop computers.[2].

Data breach notification standards are clearly a relevant concern for the millions of users sharing information through the Internet and for information being stored in various forms. Yet, with the increasingly mobile and decentralized nature of our economy and data storage and dissemination technologies, there is a growing and exceptionally strong case to be made for the creation of a national data breach notification framework that supersedes state data breach laws. Such an approach will bring clarity and certainty to consumers who may not be aware of the notice obligations of a particular state DBN law or even when such obligations may apply. For SMB's the issue of DBN reform is especially important because many of these firms do not have the requisite in-house expertise to thoroughly understand all 46 state DBN laws. Streamlining this process promotes robust compliance and serves as an incentive to SMB's to expand their businesses across jurisdictions.

Today, there are 46 states, not including the District of Columbia, Guam, Puerto Rico and the Virgin Islands, that have enacted data breach notifications laws. This patchwork of state DBN laws creates significant compliance obligations since no two state data breach laws are exactly the same. Moreover, many of these state DBN laws are in conflict with each other. State DBN laws vary as to when a data breach notice is triggered, the timeline within which notice must be provided, and rules that outline the information that must be contained in the actual notice.

Some state DBN laws require prima facie notice to the consumer when a company is made aware of a breach. Other state DBN laws require notice only if the breached data has the likelihood of resulting in harm to the consumer. State DBN laws also differ on the type of penalties and fines that can be imposed and whether a consumer can file a private right of action against a company that has suffered a breach of a consumer's personally identifiable information (PII).

For example, what happens when a Massachusetts resident traveling out of state shares, through use of his or her mobile device, personally identifying information with a local or regional business where they are visiting, and the business subsequently suffers a data breach. Under the Massachusetts state's DBN the consumer notice requirement applies to " a person or agency that maintains, stores, owns or licenses personal information about a resident of the Commonwealth."[3] As a result, any business across the United States that suffers a data breach containing PII belonging to a Massachusetts resident is in violation of the Massachusetts data breach law if it fails to comply with the notification requirement. This is true even if the business complies with its own state data breach notification requirement.

---

[2] http://www.businessinsider.com/more-mobile-devices-than-people-2013-2; http://www.computerworld.com/s/article/9219932/Most_will_access_Internet_via_mobile_devices_by_2015_IDC_says.

[3] Mass. Gen. Laws Ann. ch. 93H, §§ 1–6 (2007), Mass. Gen. Laws Ann. ch. 93A, § 4 (2007)

Public Advocacy
515 2nd St NE
Washington, DC 20002
202-503-3624

More specifically, if a Massachusetts resident happens to share their PII via a mobile device with a local business while traveling in Florida then the conflicting data breach rules become much more complicated. Under Florida's DBN law, a consumer data breach notice is not required "if, after an appropriate investigation or after consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed."[4] It should also be noted that these problems are also present when consumers access a website from their place of residence and the business is located out of state. The issue of conflicting state DBN laws still persist.

There are countless other examples that we can share that highlight the huge regulatory compliance burden imposed upon businesses due to the patchwork of conflicting state data breach notification requirements. Since each state has different notice obligations, the average consumer who becomes the victim of a PII breach faces a herculean task tracking down where the breach occurred and whether he or she should expect notice from a business with the details of the leak. Simply from a consumer protection standpoint, a federal standard would provide greater piece of mind with respect to one's PII.

These compliance obligations are particularly burdensome, however, for the small to medium size business. For example, many of CompTIA's members are comprised of just a couple of employees with very specific IT skills and core competencies.

To be clear, CompTIA fully supports the requirement that consumers receive notice when their PII has been breached. The real issue is that data breach notice obligations should not put SMB's at an economic and regulatory disadvantage as compared to larger and better-capitalized companies. The cost of complying with 46 state DBN conflicting laws places a disproportionate financial impact on SMB's.

An annual report by the Ponemon Institute (and sponsored by Symantec) found that the organizational cost for a data breach event is on average $5.4 million and the cost to an organization for a single breached record is on average $188.[5] Many of the costs associated with data breaches results from legal and regulatory liabilities.

SMB's must hire lawyers and expend other resources simply to track down the various compliance obligations. With our increasingly mobile economy the application of these laws are getting even more complicated to understand since it is not always clear about

---

[4] Fla. Stat. Ann. § 817.5681 (2005).

[5] http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-global-report-2013.en-us.pdf

the geographic boundaries of where a data breach may have actually occurred which can be different from where a consumer may actually reside.

Therefore, CompTIA believes that the creation of a national framework for data breach notification can go a long ways towards promoting effective consumer notice, reducing costs and eliminating barriers to entry for SMB firms. A national framework for data breach notification can serve as an incentive toward the expansion of IT services across state lines. For instance, when an IT firm considers expanding its business across state lines it must take into account the state regulatory and compliance obligations. A national framework for data breach notification would provide regulatory relief from that obligation.

Any national data breach notification framework should incorporate the following principles, which we also believe would receive broad industry support:

1. Preemption of State Legislation – There should be a single national federal standard for Data Breach policy. Businesses which conduct commerce over multiple states need the certainty and efficiency that a national standard would provide.

2. Technology-Neutral policy – Congress and the FTC should not mandate specific technology or methods for data security practices. The environment for data security is constantly evolving, so any regulation should focus on promoting validated industry standards for security, rather than a single quickly-outdated solution.

3. Exemption from notification requirement for entities that deploy technology/methods such as encryption and other technologies that render data "unusable or unreadable" by hackers as a harm-prevention measure.

4. No Private Right of Action for individuals seeking litigation. All enforcement and penalties for Data Breach law should be administrated by a central government agent instead of state Attorneys General, except in cases where the federal agent can or has not acted.[6]

5. Focus on gaps in coverage - Entities compliant with existing Data Breach legislation (Ex. Gramm-Leach-Bliley) should be exempt from new regulation. Do not reinvent the wheel, or create conflicting and overlapping regulations.

[6] CompTIA believes that the industry will not support criminal prosecution for "negligent" actions.

6. Avoid over-notification of consumers – Notification should occur on a "reasonable timeframe," which includes allowances for risk assessment and any necessary law enforcement procedures or investigation. Notification should be focused on events where there is a possibility of "actual harm." Possibility of including a minimum threshold of affected individuals.

Thank you again for the opportunity to share our perspective on the issue of data breach notification reform, and I would be happy to answer any questions.

Computing Technology Industry Association (CompTIA)
Public Advocacy
515 2nd St NE
Washington, DC 20002
202-503-3624

Mr. TERRY. Thank you very much.

Mr. Greene, you are now recognized for 5 minutes.

STATEMENT OF JEFFREY GREENE

Mr. GREENE. Chairman Terry, Ranking Member Schakowsky, members of the subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation. We are the largest security software company in the world with 31 years of experience in developing Internet security technology.

For organizations that have critical information assets, the risk of a data breach has really never been higher than it is now. We estimate that last year, there were 93 million identities exposed. Thankfully, few of these victims will have his or her identity stolen or bank account raided, but the reality is that all of them are at risk for it because once your information has been stolen, you can do little more than hope that no one tries to monetize it.

The costs of these breaches is real. Mr. Chairman, as you mentioned in 2012, our Norton cyber crime report put the global price tag of consumer cyber crime at $110 billion, and that is just the consumer side. On the business side, the Ponemon Institute estimated that in 2012, the average organizational cost for a breach in the United States was $5.4 million.

Breaches can be caused most commonly or very commonly by lost computers or portable media, and they can be caused by outright theft—people that walk out the door with sensitive information, disgruntled or fired employees. But there is another cause for breaches, and that is targeted attacks, and actually last year, according to our Internet Security Threat report, 40 percent of breaches were caused by targeted attacks and hackers. Most of these attacks rely on social engineering, basically trying to trick people into doing something on their computer that they were never do if they were fully cognizant of their actions. We also saw a lot of email attacks. It is still a very common vector. And we regularly see criminals mining social media to come up with tidbits about individuals they use to craft emails that will look legitimate, even to very cautious users. Twenty twelve also saw the emergence of what we call watering hole attacks. Like the proverbial lion in the jungle who waits by the watering hole for unsuspecting prey, cyber criminals have become adept at compromising legitimate Web sites and then sitting on them and waiting for visitors to come by and then attempting to compromise every one who visits.

The growing use of the cloud also presents unique challenges and opportunities. Cloud done right is an opportunity for very strong security. You are putting your data behind higher walls and having it watched by more walls. Cloud done wrong, though, can be a recipe for data breach because you are grouping your data with many other people's, creating a very desirable target for attackers and one that is not well defended.

As you mentioned, Mr. Chairman, mobile devices require strong security. We are all doing more and more of our lives on mobile computers, and unfortunately, the criminals are following. Last year, we saw a 58 percent increase in the types of malware that were designed specifically for mobile devices, and even since we re-

leased our report in April, we have seen dramatic evidence of the increasing focus on mobile attacks.

Good security really starts with the basics—patch management, updating your patches on your computer, and strong passwords. The breach that the ranking member indicated was reported this morning, based on the early reporting, there was a significant number of people who were using the word "password" as their password. That is just not a strong password; you are asking for it.

So-called zero days or previously unknown critical vulnerabilities receive a lot of media attention, but unfortunately, it is still well-known older vulnerabilities that cause most patches. Modern security software is essential. I am not talking about the proverbial your father's antivirus anymore. Modern security software will monitor your computer looking for anomalous Internet activity, processes or other system events that could be indicative of a previously known infection. We have reputation-based technology we use that actually looks at individual files based upon their frequency we see out in the wild and we are able to detect previously unknown threats just by looking at a file that way.

Looking at the legal landscape, we do support a national standard for breach notification, and we have identified three principles that are key to us. First, the scope of any legislation should include all entities that collect, maintain or sell significant numbers of records containing sensitive personal information, and we think that that should apply equally to the government and to the private sector. Second, pre-breach security measures should be central to any legislation. New legislation should seek to minimize the likelihood of a breach and not just focus on what to do afterward. And finally, any notification scheme should minimize false positives. Promoting technology like encryption as a best practice would significantly reduce these false positives and limit the burden on consumers and on businesses.

I thank you again for the opportunity and the privilege to testify today. I look forward to your questions.

[The prepared statement of Mr. Greene follows:]

Prepared Testimony and
Statement for the Record of

Jeffrey E. Greene
Senior Policy Counsel, Cybersecurity and Identity
Symantec Corporation

Hearing on

"Reporting Data Breaches:
Is Federal Legislation Needed to Protect Consumers?"

Before the

U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing and Trade

July 18, 2013

2123 Rayburn House Office Building

Chairman Terry, Ranking Member Schakowsky, distinguished members of the Subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Jeff Greene, and I am the Senior Policy Counsel for Cybersecurity and Identity at Symantec, where I focus on cybersecurity, identity management, and privacy issues. I currently serve as vice-chair of the Homeland Security Committee of the American Bar Association's Section of Science & Technology Law and co-chair of the Supply Chain Working Group of the Information Technology Sector Coordinating Council. Prior to joining Symantec, I was Senior Counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where I focused on cybersecurity and Homeland Defense issues. I have also worked on the Committee on Homeland Security in the House of Representatives as a subcommittee staff director and as counsel to the Senate's Special Investigation into Hurricane Katrina. Before that, I was Counsel to a Washington, D.C. law firm, where my practice focused on government contracts and contract fraud, as well as general civil and criminal investigations.

Symantec is the largest security software company in the world, with over 31 years of experience developing Internet security technology. We provide security, storage, and systems management solutions to help consumers and organizations secure and manage their information and identities. Our Global Intelligence Network (GIN) is comprised of more than 69 million attack sensors in over 200 countries, and records thousands of events per second. In addition, every day we process more than three billion e-mail messages and more than 1.4 billion web requests across our 14 global data centers.

These resources allow us to capture worldwide security intelligence data that gives our analysts a view of the entire Internet threat landscape, including emerging cyber attack trends, malicious code activity, phishing, and spam. We welcome the opportunity to provide comments as the Subcommittee continues its important efforts to bolster the state of data security in the US. In my testimony today, I will discuss

- Some recent statistics on data breaches;
- How the breaches are happening, including the methods and tactics criminals currently use to steal data;
- Some basic security measures individuals and companies can employ; and
- Key elements to any legislative solution for addressing data breaches.

Data Breaches by the Numbers

For organizations that have critical information assets such as customer data, intellectual property, trade secrets, and proprietary corporate data, the risk of a data breach is now higher than ever before. Some metrics:

- We estimate that there were 93 million identities exposed in 2012 (in 2011 there were 232 million)[1];
- The average breach involved data for 605,000 individuals (down from 1.1 million in 2011)[2];

[1] *Symantec Internet Security Threat Report* XVIII (April 2013), 17. http://www.symantec.com/security_response/publications/threatreport.jsp

- There were fewer massive data breaches in 2012, but there were more smaller ones[3];
- The median number of identities compromised per incident was 8,350 (more than 3x the 2011 median of 2,400)[4]; and
- Hacktivism – which was a major driver of breaches in 2011 – diminished as a factor in 2012;

Of course, these numbers are cumulative – once an identity has been exposed, it does not get "unexposed" when the calendar changes. So in the most basic of terms, as a result of breaches in 2011 and 2012 alone, the personal information of 325 million individuals is or could be for sale on the criminal black market to be used for identity theft, credit card fraud, and countless other illegal activities.

To be clear, not every one of these victims will have his or her identity stolen or bank account raided. In fact, a low percentage of them will actually suffer that kind of direct loss. But every one of them is at risk for it because once your personal information is outside your control, you can do little more than hope that no one tries to monetize it either by using it themselves or selling it on the thriving black market. If your computer was compromised either as the source or as a result of a breach, until you are aware of it and are able to clean your system you are entirely at the mercy of the criminals. Your computer could be used to steal from you, or as part of a network of compromised computers that can send spam, take part in a denial of service attack, or try to infect other computers.

The cost of these breaches is very real and is borne directly both by companies and consumers:

- In our 2012 Norton Cybercrime report, we put the global price tag of consumer cybercrime at $110 billion annually[5];
- We estimate that there are 556 million victims of consumer cybercrime per year (1.5 million victims per day, 18 per second)[6];
- On the business side, the Ponemon Institute estimates that in 2012, the cost to US companies was $188 per identity compromised[7];
- Ponemon's survey concluded that the average total organizational cost of a breach in 2012 was $5.4 million[8]; and
- Attackers are increasingly targeting smaller businesses, 71% of whom say their operations are somewhat or very dependent on the Internet.[9]

There is reason to be hopeful, however. The Ponemon survey found that an ounce of prevention is indeed worth a pound of cure. Strong security protocols before a breach and good incident

---

[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *2012 Norton Cybercrime Report* (September 2012), 6. http://www.norton.com/2012cybercrimereport
[6] *Id.* at 23.
[7] *Cost of Data Breach Study: Global Analysis,* Ponemon Institute (May 2013), 1. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013
[8] *Id.* at 1.
[9] *Symantec 2012 National Small Business Study Fact Sheet*, National Cybersecurity Alliance & Symantec Corporation, 1. http://www.staysafeonline.org/stay-safe-online/resources/

management policies should a breach occur significantly decreased the average breach cost. Similarly, more consumers than ever are taking basic security measures such as deleting suspicious emails and using security software.

How Data Breaches are Occurring

While the continuing onslaught of data breaches is well documented, what is less understood is why data breaches happen and what can be done to prevent them. The main causes for breaches are human error, system problems, and targeted attacks.

Company employees who violate data security policies still cause a large number of data breaches. Even today, employees work with sensitive information on unprotected servers, desktops, and laptops; in many ways, this is the natural result of a highly productive workforce. One of the most common types of data breach occurs when well-meaning insiders do not encrypt the sensitive data that they store, send, or copy. If a laptop is lost or stolen – or a hacker gains access to a network – these files are completely unprotected. And while most companies have policies that require encryption or other security precautions for sensitive data, many employees either ignore or do not know about the policies.

Email, web mail, and removable storage devices are another major source of breaches. Most of us at one time or another have emailed something to our home address from our office so that we can work on it later. If our email accounts or home computers are compromised, or if we misplace the thumb drive we use to transport files, any sensitive, unencrypted data we sent is now lost and our company has had a data breach. Data breaches can also be caused by outright theft – a fired or disgruntled employee who steals sensitive information.

There is of course another cause for data breaches – targeted attacks. According to our 2013 Internet Security Threat Report (ISTR), 40% of data breaches were caused by hackers.[10] Some are direct attacks on a company's servers, where attackers search for unpatched vulnerabilities on websites or undefended connections to the internet. But most rely on social engineering – in the simplest of terms, trying to trick people into doing something that they would never do if fully cognizant of their actions. Email is still a major attack vector and can take the form of broad mailings ("phishing") or highly targeted messages ("spear phishing"). More and more we see the latter variety, with publicly available information used to craft an email designed to dupe a specific victim or group of victims. The goal of both varieties is to get victims to click on a link to a website that will then try to infect their computers or to open infected documents that will do the same. While good security will stop most of these attacks – which often seek to exploit older, known vulnerabilities – many companies do not have up-to-date security or have it unevenly applied throughout their workforce.

Social media is an increasingly valuable tool for cyber criminals. It is particularly effective in direct attacks, as people tend to trust things that appear to come from a friend's social media feed. But social media is also widely used to conduct reconnaissance for spear phishing or other highly targeted attacks; it often provides just the kind of personal details that a skilled attacker can use to get a victim to let his

[10] *ISTR XVIII*, 19.

or her guard down. The old cliché is true when it comes to cyber attacks: we have to be right 100% of the time while the attacker only has to get it right once.

In 2012, we also saw the rapid growth of "watering hole" attacks. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cyber criminals have become adept at lying in wait on legitimate websites and using them to try to infect visitors' computers. They do so by compromising legitimate websites that their victims are likely to visit and modifying them so that they will surreptitiously try to deliver malware to every visitor. For example, one attacker targeted mobile app developers by compromising a site that was popular with them. In another case, we saw employees from 500 different companies visit one compromised site in just 24 hours, each running the risk of infection.[11] Cyber criminals gained control of these websites through many of the same tactics described above – spear phishing and other social engineering attacks on the site managers, developers, or owners. Many of these websites were compromised through known attack vectors, meaning that good security practices could have prevented them from being compromised.

All of these attacks have essentially one goal: to get control of the user's computer. In an intrusion into a company, once inside, attackers will typically conduct reconnaissance of the system and then move laterally within it until they find what they want to steal. In the case of an attack on an individual, the criminal will install malicious software ("malware") that allows them to steal information or otherwise take control of the computer for future use.

How to Protect Your Data

When it comes to security, it starts with the basics. Though criminals' tactics are continually evolving, good cyber hygiene is still the simplest and most cost-effective first step. Strong passwords remain the foundation of good security – on your email, your social media accounts, whatever you use to communicate or really anything you log into. And these passwords must be different, because using a single password means that a breach of one account exposes all your accounts.

Patch management is also critical. Do not delay installing patches, because the same patch that closes a vulnerability on your computer can be a roadmap for a criminal to exploit it and to compromise any unpatched computers. The reality is that a large percentage of computers around the world do not get patched regularly, and cyber criminals count on this. While so-called "zero days" – previously unknown critical vulnerabilities – get the most press, it is older, un-patched vulnerabilities that cause most systems to get compromised.

A modern security suite is essential too. While most people still commonly refer to security software as "anti-virus," good security needs to be much more than that. In the past, the same piece of malware would be delivered to thousands or even millions of computers. Today, cyber criminals can take the same malware and create unlimited unique variants that can slip past basic anti-virus software. Modern security software will monitor your computer, watching for unusual internet traffic, activity, or system processes that could be indicative of malicious activity. At Symantec we also use what we call Insight,

[11] *Id.* at 21.

which is a reputation-based security technology that puts files in context, using their age, frequency, location and more to expose threats that might otherwise be missed.

The move to the cloud presents both opportunities and challenges. Cloud done right is a huge boon for security – you are putting your data behind more secure walls and leveraging the knowledge and the resources of a broader community to protect yourself better. Cloud done wrong is a recipe for a data breach – you are putting all of your vital information in a place that is attractive to attackers yet poorly secured. The non-profit Cloud Security Alliance promotes the use of best practices for providing security in the cloud, and has published a matrix of security controls that provide a good baseline for any provider. Symantec is one of the largest cloud providers in the world, and we marry our cutting edge security technology with cloud services to create a secure on-line environment.

Mobile devices require security too, for as we conduct more of our online lives on mobile devices, the risks will increase accordingly. Cyber criminals will go where the money is, and we are already seeing them shift their focus to mobile. As we reported in the 2013 ISTR, there was a 58% increase in families of mobile malware over the previous year, and that trend shows no sign of slowing down.[12] Since the ISTR was released in April, we have seen further evidence of the shift to mobile attacks, as more malware that was originally designed for PCs has been adapted for use against mobile devices. As with PCs, the solutions are not complex: practice good hygiene and use security software where available.

Encryption is also key to protecting your data. Even the best security will not stop a determined attacker, and encrypting your sensitive data provides defense in breadth. Good encryption ensures that any data stolen will be useless to virtually all cyber criminals. The bottom line in computer security is no different from physical security – nothing is perfect. We can make it hard, indeed very hard, for an attacker, but if resourced and persistent criminals want to compromise a particular company or site, with time they are probably going to find a way to do it. Good security means not just doing the utmost to keep them out, but also to recognize that you must take steps to limit any damage they can do should they get in.

Data Breach Laws

Today there are at least 48 state-specific data breach notification laws. This creates an enormous compliance burden, particularly for smaller companies, and does little to protect consumers. Symantec supports a national standard for data breach notification, built on three principles:

1. Data security legislation should apply equally to all. The scope of any legislation should include all entities that collect, maintain, or sell significant numbers of records containing sensitive personal information. Requirements should impact government and the private sector equally, and should include educational institutions and charitable organizations as well. By the same token, any new legislation should consider existing federal regulations that govern data breach for some sectors and not create duplicative, additional, or conflicting rules.

[12] *Id.* at 34.

2. Implementing pre-breach security measures should be central to any legislation. As the Ponemon survey demonstrates, breaches are much less costly for companies that are proactive. New legislation should not simply require notification of consumers in case of a data breach, but should seek to minimize the likelihood of a breach by requiring reasonable security measures to ensure the confidentiality and integrity of sensitive personal information.

3. The use of encryption or other security measures that render data unreadable and unusable should be a key element in establishing the threshold for the need for notification. Any notification scheme should minimize "false positives." A clear reference to the "usability" of information should be considered when determining whether notification is required in case of a breach. Promoting the use of encryption as a best practice would significantly reduce the number of "false positives," thus reducing the burden on consumers and business.

Conclusion

The good news is that people are getting smarter. Our 2012 Norton Cybercrime Report showed that 89% of people will delete suspicious emails, 83% have basic antivirus, and 78% do not open attachments or links in unsolicited emails or texts.[13] That is a significant improvement from a few years ago, and a positive trend. Similarly, it is increasingly clear that strong security before a breach occurs and well-developed incident management policies to deploy after a breach can decrease the damage that a breach will cause to an organization.

The bad news is that the criminals know this, and they modify their techniques accordingly. That is why your hearing today and your focus on this important issue could not be more timely. Thank you again for the opportunity to testify, and I am happy to answer any questions you have.

[13] *2012 Norton Cybercrime Report*, 16.

Mr. TERRY. Thank you very much.
Ms. Matties, you are recognized for 5 minutes.

STATEMENT OF DEBBIE MATTIES

Ms. MATTIES. Chairman Terry, Ranking Member Schakowsky, and the members of the subcommittee, thank you for the opportunity to participate in today's hearing. My name is Debbie Matties, and I am the Vice President for Privacy at CTIA.

CTIA along with AT&T, Comcast, DIRECTV, NCTA, Time Warner Cable, USTelecom, and Verizon is a member of the 21st Century Privacy Coalition. The Coalition seeks to modernize U.S. privacy and data security laws to better serve consumers as well as to reflect the ways that communications technology and competition has changed in the last two decades.

CTIA commends the subcommittee for exploring whether federal data breach legislation is necessary to protect consumers. Today's patchwork of state and federal data security and breach notification laws is complicated for businesses and provides uneven protection for consumers. A strong, comprehensive and streamlined federal framework enforced by a single agency would create more certainty for businesses and better protect consumers from the harms associated with data breaches.

Today's variety of State and federal requirements creates inconsistent, sometimes contradictory responses to breaches that do not benefit consumers. For example, some States require breach notifications to occur "without unreasonable delay" whereas other States require specific time frames for notification. Some states provide an exemption for notification for immaterial breaches whereas other States do not.

Most data breaches impact consumers in multiple States, just like the breach that happened here in the House, and electronic data is rarely segmented by State. So under law, the question becomes, which State law should apply? The State in which the consumer resides? The State in which the breach occurred or the State in which a vulnerability existed and was exploited? For wireless consumers using family plans, often the user of a device is in a different State from the subscriber who pays the bill. Given the fact that breaches inevitably transcend State borders, a federal approach to breach notification is appropriate so that all consumers receive the same benefits.

The absence of a consistent nationwide regime also creates unnecessary distraction for companies that need to stop a breach, evaluate the damage caused by the breach and its scope, correct whatever vulnerability resulted in the breach, work with law enforcement to investigate the brief, and of course, most important, notify consumers to help mitigate any harm. These time-sensitive activities are hampered when a company, especially a small business, has to evaluate which of the 48 different State regimes applies to each of their customers and then tailor breach notifications accordingly. It also makes it difficult for consumer protection agencies, consumer advocates and businesses to educate consumers faced with a data breach about their rights.

Multiple federal regimes undermine consumer protection in a similar manner. For example, wireless carriers fall within the

FCC'S CPNI rules to the extent they are providing a telecommunications service such as voice. But some providers of voice like Skype are not subject to CPNI rules, and then the FTC asserts data security jurisdiction over wireless carriers when they are providing Internet access.

In any case, the CPNI rules don't really make a lot of sense. They don't cover critically important information like name, Social Security number or credit card number but they do cover, for example, the number of voice lines a subscriber has on her plan. A unified, streamlined federal data security and breach notification law that applies equally to all entities and to all data would make consumers more confident in the security of their online information and would in turn give them greater trust in Internet commerce. This unified federal approach to data security is bipartisan and is in line with the Obama Administration's recommendations to level the playing field for companies and provide a consistent set of expectations for consumers by simplifying and clarifying the privacy laws. CTIA supports the Administration's recommendation to narrow the common carrier exemption to the extent needed to enable the FTC to enforce data security and data breach notification requirements.

Mr. Chairman, CTIA fully supports a unified, streamlined federal data security and breach notification law that is enforced by the FTC and benefits consumes who expect that their information will be afforded the same high degree of protection regardless of what entity collects the information, where the consumer lives, where a breach occurs, or where hackers may be trying to access personal information. Congress should enact a new law to better reflect consumer expectations.

I would be happy to answer your questions.

[The prepared statement of Ms. Matties follows:]

Testimony of

Debbie Matties

Vice President, Privacy

CTIA – The Wireless Association®

on

"Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?"

before the

House Energy & Commerce

Subcommittee on Commerce, Manufacturing, and Trade

July 18, 2013

Chairman Terry, Ranking Member Schakowsky, and other Members of the Subcommittee, thank you for the opportunity to participate in today's hearing on behalf of CTIA – The Wireless Association®. My name is Debbie Matties, and I am the Vice President for Privacy at CTIA. Before joining CTIA, I served as an Attorney Advisor for Consumer Protection to former Federal Trade Commission Chairman Jon Leibowitz.

CTIA, along with AT&T, Comcast, DIRECTV, Time Warner Cable, United States Telecom Association and Verizon, is a founding member of the 21st Century Privacy Coalition (the Coalition). The Coalition was formed to advocate for modernization of U.S. privacy and data security laws to better serve consumer expectations as well as to reflect technological and competitive changes in the communications marketplace.

CTIA commends the subcommittee for exploring whether federal data breach legislation is necessary to protect consumers. Today's patchwork of state and, in certain sectors, federal information security and data breach notification laws is often confusing to businesses and provides uneven protection for consumers. A comprehensive, streamlined federal framework enforced by a single agency would create more certainty for businesses and better protect consumers from the harms associated with data breaches.

The daily cyber-attacks on commercial networks, the increasing prevalence of malware, and ongoing criminal enterprises focused on stealing consumer financial information have resulted in high-profile security breaches that have exposed information belonging to millions of consumers.[1] When such breaches subject consumers to identity theft or other financial harm,

[1] *See* Eric Dash, *Citi Says Many More Customers Had Data Stolen by Hackers*, N.Y. TIMES (June 16, 2011), http://www.nytimes.com/2011/06/16/technology/16citi.html; Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS, Apr. 26, 2011, http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426; Laura Strickler, *Secret Service Investigates Epsilon Data Breach*, CBS NEWS (Apr. 4,

consumers need to be notified so that they can take actions to protect themselves from further harm.

Yet the patchwork of state, and even federal, information security and data breach notification requirements creates inconsistent, sometimes contradictory responses to breaches that do not benefit consumers. For example, some states require breach notifications to occur "without unreasonable delay," whereas other states require specific timeframes for notification. Some states provide an exemption from breach notification for immaterial breaches, whereas other states do not. Most states provide an exemption from breach notification if consumers' information is encrypted, but other states do not.[2]

The absence of a consistent nationwide regime creates an unnecessary distraction for companies that need to (1) stop a breach, (2) evaluate the damage caused by such a breach, (3) correct whatever vulnerability resulted in the breach, (4) work with law enforcement to apprise such officials of the breach, and (5) notify consumers to help mitigate any harm. But these time-sensitive activities are hampered when a company has to sift through 47 different state regimes to determine procedures for breach notification.

Electronic information is rarely, if ever, segmented by state, so a breach invariably impacts consumers in multiple states. Because breaches often transcend state boundaries, which state law should even apply – the state in which the consumer resides, the state in which the breach occurred, or the state in which a vulnerability existed and was exploited – is often

---

2011), http://www.cbsnews.com/8301-31727_162-20050575-10391695.html. *See generally* Stephen Grocer, *Sony, Citi, Lockheed: Big Data Breaches in History*, WALL ST. J. (June 9, 2011), http://blogs.wsj.com/deals/2011/06/09/sony-citi-lockheed-big-data-breaches-in-history.

[2] *Compare* CAL. CIV. CODE § 198.29(a) (providing exception for encrypted data), *and* ARIZ. REV. STAT. ANN. § 44-7501(a) (2007) (West) (same), *with* WYO. STAT. ANN. § 40-12-502 (West 2007) (proving no exception for encrypted data).

unclear. Given the fact that breaches transcend state boundaries, a federal approach to breach notification is appropriate so that all consumers receive the same benefit. Multiple federal regimes undermine consumer protection in the same manner as multiple state regimes. For example, wireless carriers are subject to the Federal Communications Commission's Customer Proprietary Network Information (CPNI) rules to the extent that they are providing a telecommunications service, such as voice service.[3] But wireless carriers are subject to Federal Trade Commission data security enforcement to the extent that they are providing an information service, such as Internet access.

Even more confusingly, location information that can be collected from a consumer's mobile device is subject to the Federal Communications Commission's CPNI rules if "the collection is undertaken at the carrier's direction and that the carrier or its designee has access to or control over that information."[4] But this requirement does not apply if the location information is simply collected by an application not at a carrier's direction or under a carrier's control.[5]

Consumers do not expect the data security rules that apply to location information to differ based upon the entity collecting such information; consumers expect the same rules to apply to the same information. Consumers use a range of functionally equivalent services and applications, often on the same communications platform. These services and applications

---

[3] *See* 47 U.S.C. § 222 (2008).

[4] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, CC Docket No. 96-115, at ¶ 16 (rel. June 27, 2013).

[5] In addition to uneven federal protection for consumers, federal data security and date breach notification rules to which telecommunication providers are subject do little to protect consumers from identity theft. The CPNI definition leaves out personal information like credit card numbers, but protects non-sensitive information, such as services a subscriber has ordered.

collect the same type of information, and consumers expect that the same information security standards will apply.

Consumers would greatly benefit from a unified, streamlined federal data security and breach notification regime that applies equally to all entities. Such a regime would make consumers more confident in the security of their online information, which would give them greater trust in their use of the Internet.

CTIA agrees with the Obama Administration's recommendation that "because existing Federal laws treat similar technologies within the communications sector differently, the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers."[6] CTIA also supports the Administration's recommendation that a federal framework "provide a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency in the basis for FTC enforcement actions."[7] That should apply not only to telecommunications carriers currently subject to the CPNI requirements, but also to cable and satellite operators subject to data breach requirements in Sections 631 and 338 of the Communications Act of 1934, respectively.[8] Under such a framework, CTIA supports a narrowing of the common carrier exemption to enable the Federal Trade Commission (FTC) to enforce information security and data breach notification requirements.

---

[6] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 39 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[7] *Id.* at 36.

[8] *See* 47 U.S.C. § 551, § 338(i).

In addition, a unified, streamlined federal data security and breach notification regime should only be enforced by the Federal Trade Commission; it should not include a private right of action. The data security and breach notification regimes of at least 15 states include a private right of action. Some trial lawyers have sought to leverage these requirements against companies that are the subject of a data breach to obtain monetary awards that are not tied to consumer injury and that often do not benefit consumers.[9] Even when no wrongdoing has occurred, companies often bear great expense going to trial under these laws.[10] A law enforcement regime will result in better compensation for consumers who have been injured.

Thank you again for the opportunity to present CTIA's views at today's hearing. CTIA fully supports a unified, streamlined federal data security and breach notification regime that is enforced by the FTC and applies to all entities. Consumers expect that their information will be afforded the same degree of protection, regardless of the entity collecting the information and of the State in which the consumer resides. A federal framework would give consumers greater confidence that the safety of their online information will be afforded the same degree of care regardless of where they live, where a breach occurs, or where hackers may be trying to access their information. Congress should enact a new law to better reflect consumer expectations.

---

[9] *See, e.g., Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *1-2 (S.D.N.Y. June 25, 2010) (collecting dozens of class actions where plaintiffs "claim to have suffered little more than an increased risk of future harm from the loss (whether by accident or theft) of their personal information"); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011) ("Here, no evidence suggests that the data has been—or will ever be—misused.").

[10] *See* Sasha Romanosky *et al.*, *Empirical Analysis of Data Breach Litigation, Research Paper No. 2012-29, in* Temple Univ. Beasley Sch. of Law Legal Studies Research Paper Series (Gregory Mandel & Shyam Nair, eds., 2012), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461 (finding that defendants settle 49% of data breach lawsuits without allegations of actual harm and theorizing that defendants "may be rationally choosing to settle to avoid further litigation costs, publicity, or business distraction").

Mr. TERRY. Well done.

Professor Matwyshyn, you are now recognized for 5 minutes.

STATEMENT OF ANDREA MATWYSHYN

Ms. MATWYSHYN. Thank you. Chairman Terry, Ranking Member Schakowsky, it is my great honor to be with all of you today to discuss a topic that I have devoted my scholarship to, and that is the question of how to improve information security in the United States.

I started working in this space approximately 14 years ago as a corporate attorney representing multinational clients as well as entrepreneurs in Chicago. I really watched the evolution of this space as both a member of the business community at first representing clients and now as an academic, and although there has been tremendous improvement in this space, we still have a reasonable way to go.

The public awareness around questions of information security has tremendously increased during the last 10 years, and it is with great pleasure that I see that we are discussing these topics today. However, the questions of conduct and reasonableness in behavior and information security still remain unanswered.

With that, I would like to offer a historical example to offer perhaps a paradigm to conceptualize questions of information security. In addition to teaching Internet law and data security and privacy law, I also teach securities regulation, and I would submit that perhaps the questions that we are facing today have a historical parallel in the questions that this Congress faced when thinking about balancing the interests of consumer protection, capital formation and market stability in the 1933 and 1934 Acts.

Today in this context, perhaps those three elements are consumer protection, economic stability broadly in terms of securing information and preserving sectors of our economy that rely on information flows, and facilitating responsible innovation. So with those three elements, we can take a look at the broader set of questions in information security, and I would submit that perhaps we should draw a clear distinction between disclosure regulation and conduct regulation.

Disclosure regulation, specifically data breach notification statutes, have developed to a high degree on the State level. We have had States function as the laboratories of experimentation, and the State statutes have shown us the way as to what is a feasible and successful approach for disclosure, and offered us guidance to at this point be able to come up with a set of criteria that can be operationalized on a national level through the Federal Trade Commission to provide us the data to be able to analyze what is going on in our economy, who are the companies that are behaving with best practices, and who are the companies that are not yet quite up to par and need to be encouraged regulatorily or otherwise on the State or national level to improve the quality of information security that they implement throughout the their organizations. The written statement that I have submitted offers a framework of this nature.

Conduct regulation, I would submit, we are not ready to really focus in on with a national framework yet. We need the states to

show us the way, the same way that they did in the context of data breach notification. Let the states experiment, guide us, discover what works, what doesn't work, and then perhaps we can revisit this question. I would respectfully urge this body to allow for this state experimentation and to preserve the right of states to determine recourse appropriate for their consumer harms.

While disclosure legislation deals with purely providing information to empower consumers to make good choices, conduct regulation is the place where we contemplate harms. This distinction, I think, would be fruitful to operationalize into a national framework for a data breach notification harmonization.

And in my last minute, I will highlight some of the elements that I elaborate on in detail in my written statement that may provide guidance for a federal harmonized framework.

First, the concept of information from a consumer and from a corporate perspective does not map onto the notion of PII that we have been working with. Sometimes the most innocuous bits of information can be the most important. If I use my favorite flavor of ice cream as my security question for my bank account, that is perhaps my most sensitive information, and so I would suggest that perhaps we should reconceptualize our notion of what constitutes consumer information in line with the way that sophisticated companies treat information and that is around information that is shared by a consumer in a trusted relationship.

And with that, I will conclude because I am running out of time but I would request that this committee turn to my statement and examine the framework that I have proposed. Thank you.

[The prepared statement of Ms. Matwyshyn follows:]

Statement of Dr. Andrea M. Matwyshyn
Assistant Professor, Legal Studies and Business Ethics, The Wharton School, University of Pennsylvania/ Affiliate, Center for Technology, Innovation and Competition, University of Pennsylvania Law School/ Affiliate Scholar, Center for Internet and Society
Stanford Law School

Before the
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives
July 18, 2013

Chairman Upton, Ranking Member Waxman, and distinguished members of the Committee, it is my honor to be here with you today to discuss the future of data security regulation in the United States. My testimony today reflects my academic work and the cumulative knowledge that I have acquired during the last fourteen years as a corporate attorney and academic researching and studying the legal regulation of data breaches and information security policy. It further reflects practical knowledge obtained through long-standing relationships with insiders at Fortune 100 technology companies, consumer rights advocates, and independent information security professionals. The proposals I offer today reflect my consultations with experts in each of these impacted communities.

During the last decade, awareness of information security has dramatically increased among both consumers and companies, and state data breach notification statutes have contributed to this improvement. However, the field of information security is still in its early years, and the overall level of information security knowledge and care that currently exists in the United States is unsustainably poor. Consumer confidence in the data stewardship capabilities of both companies and government agencies is eroding, and dramatic information security improvements are necessary throughout the public and private sector. It is this context that frames the legal and policy conversation around data breach notification.

- The dominant objections from the business community with respect to the current state-level data breach notification regime arise from definitional ambiguities and interstate variation in regulatory filing requirements. Both objections can be resolved through a federal paradigm that (1) clearly defines a reportable breach as the unauthorized access of *any* protected information connected with a consumer login credential and (2) offers a centralized, publicly available Federal Trade Commission-managed filing registry. This approach simultaneously cuts compliance costs and provides efficient notice to regulators and consumers.
- A legal distinction should be drawn between data breach disclosure regulation and information security conduct regulation. Federally streamlining data breach notification should not preempt states' rights to regulate information security conduct - both with respect to sanctions for a failure to disclose or correctly notify consumers and with respect to inadequacy of information security measures.

- Limiting states' rights to impose liability for information security misconduct will further erode consumer trust and damage innovation in the United States.

* * *

Fortune 100 corporate executives tasked with data breach notification compliance have repeatedly voiced two dominant concerns regarding their compliance experiences with state data breach notification statutes – (1) definitional ambiguities and variation in state statutes around which information triggers a breach notification and (2) inconsistent filing requirements across state level agencies. As such, should Congress wish to author a federal data breach notification law, I propose a four-pronged approach.

(1) Reframe notification around a straightforward bright line rule - unauthorized access to consumer login credentials or any protected consumer-connected information.

Because of the definitional ambiguities around which types of "information" compromise trigger breach notification, a streamlined norm is emerging among the most sophisticated technology companies: when a consumer login credential[1] or *any* previously protected data connected with a consumer may have been accessed by an unauthorized individual, these sophisticated information technology companies are erring on the side of data breach notification. Although this standard may reach above the standards demanded by most current state level statutes, in practice, it is a more cost-efficient compliance standard. It creates a bright-line rule that intuitively maps onto logical structuring of information security measures inside the company.[2] Also, because this bright line rule of notification is consistent with widespread technology practices, reports by digital forensic investigators can serve as the primary basis for breach notification filings and require less supervision (and expense) of legal counsel.

Companies understand this bright line – it maps onto the way they value the information themselves. Information value is created through a combination of scarcity and context. Specifically, companies that license databases of consumer information create value by protecting and only selectively disclosing their information. The rarer a particular piece of information, the more potentially valuable it is. Perhaps counterintuitively, consumer information that may seem superficially irrelevant, such as my favorite flavor of ice cream, may in reality be my most valuable information. For example, a consumer may use her favorite flavor of ice cream as her security question for her bank website. While this information may seem trivial on its face, the context of its use as a security question generates a tremendous value for a criminal seeking to compromise her bank account. If her favorite flavor of ice cream is the information least widely known about her and if she use it as the answer to her bank account

[1] A consumer login credential refers to a user id and password.

[2] A company engaging in prudent information security structuring of its information creates multiple technological barriers between the databases that contain consumer credentials and information and the rest of the corporate network. Specifically, when a company structures its systems in a reasonable manner to protect consumer information, the information which is bound up with login credentials is frequently redundantly protected. Best industry practices create barriers whenever possible between the sections of the network that contain consumer login credentials and derivative information and those parts of the network that do not. Thus, when an intrusion is detected, if information security measures in place are rigorous, the intruder may compromise the network more broadly but may not necessarily access consumer information. Not every security compromise will result in a data breach notification.

security question, it becomes the key to an identity thief emptying her bank account. Thus, all consumer-connected information is valuable information in data breaches and should trigger notification requirements. Treating different types of consumer information differently – government identifiers versus email addresses versus purchasing preference information – ignores this role of scarcity and context in creating valuable information. A data breach notification regime that defines a breach as the compromise of consumer login credentials or any consumer-connected information better mirrors business reality.

(2) Encryption exemptions are not useful.

Although certain states offer encryption exemptions in their statutes, these exemptions are plagued with definitional ambiguities that confound technologists and compliance personnel. They should be eliminated. Regardless of whether information is encrypted, depending on the methods and operational practices used to encrypt, it may be simple for thieves to decrypt stolen data. Compliance personnel at sophisticated technology companies believe that blanket encryptions exemption gives a pass to companies with weak security, unfairly disadvantaging sophisticated companies who invest in state-of-the-art security and implementation. Indeed, sophisticated companies now compete on quality of security.[3]

(3) Create a centralized, publicly available data breach notification registry under the Federal Trade Commission.

One of the greatest frustrations voiced by data breach compliance personnel relates to variation across state statutes in designating a state level regulator for notification: compliance personnel must file numerous forms with various different state level regulators. Through the creation of a public, national data breach notification registry maintained by the Federal Trade Commission, compliance personnel would only need to engage in one regulator notification. This centralized filing should contain, at a minimum, the following information:

a. A consumer-friendly description of the breach written in plain English
b. Date of start of breach (if known)
c. Length and extent of intrusion
d. Date of detection
e. Name and contact information of the forensic investigator/head of incident response
f. Date of consumer notification
g. Total records impacted
h. Total people impacted
i. States of residency of impacted consumers and the number of records per state
j. Manner of notice provided to consumers (written, electronic, telephone, other)
k. Services offered to impacted consumers
l. Type of attack/ technical description of breach (hacking, inadvertent disclosure, stolen or lost hardware, insider wrongdoing, other)

[3] Nevertheless, on a uniform data breach disclosure form, it would be logical to include a line item asking whether the data was encrypted and which software was used to carry out this process. Through this additional disclosure consumers and regulators will be able to assess which companies are obviously not engaging in state-of-the-art information security practices.

m. Presence of encryption and identification of the version of software used
n. Description of acquired information
o. Cause of breach
p. Description of completed or planned improvements to information security in response to the breach
q. Name and contact information for a designated individual at the company to answer consumer questions.
r. Dates of previous breach notifications in the last five years

Through the creation of a centralized data breach notification registry, appropriate state level regulators can easily access information at their discretion. Meanwhile, the compromised entity only needs to engage in a single regulatory filing, plus any direct consumer notification – a dramatically streamlined and more cost-effective process. Further, consumers will be better served than they are through the current notification regime. Reporters and data privacy advocates will be able to better identify new data breaches and analyze their severity and impact more quickly. Therefore, the regulatory purpose for data breach notification statutes -- advising consumers of the existence of a breach which may be relevant to their preservation of digital identity – would be buttressed under this proposed approach.

(4) Do not preempt enforcement authority of state regulators.

Two fundamental assumptions of the model above for the federal harmonization of data breach notification are, first, the division between disclosure regulation and conduct regulation, and, second, preserving state enforcement authority. Data breach notification obligations implicate different policy and legal questions than does an assessment of the underlying appropriateness of the security conduct leading up to the breach. These two questions should remain distinct. In many legal regimes in the United States, the notification function of filings stands distinct from any liability imposition for underlying misconduct.[4] In securities law, for example, overlapping regulatory functions exist on both the federal and state level. Multiple regulators successfully collaborate to ensure consumer protection and market stability. Just as the Securities and Exchange Commission prescribes the appropriate format for public companies' periodic filings while preserving the possibility of enforcement action by state regulators, so too the Federal Trade Commission (and any other agency that considers a need for information security disclosure to exist in specific economic sectors) can prescribe a standardized data breach notification filing form.

Just as in the securities regulation context, a clear distinction should be drawn between disclosure liability and conduct liability data security regulation. While it is logical for Congress (and state agencies) to impose fines on companies who fail to submit data breach notification filings in a timely manner,[5] these fines are fundamentally different from and disconnected from the broader questions of the reasonableness of the underlying information security conduct

[4] For example in securities regulation, publicly traded companies are required to file periodic filings offering additional information to the market with respect to their important business activities. These notification obligations carry their own penalties for failure to timely perform these statutory obligations. However, any material misstatements or omissions that may exist in the filings are governed separately under both state and federal law.
[5] Similarly it would be reasonable to impose liability for any false or omitted information in those filings

implicated in the breach. As such, while Congress may wish to at this juncture address notification harmonization, *it would be unwise and damaging to technology innovation in the United States to limit liability for information security inadequacy.* Bolstering consumer confidence in technology-mediated business requires a safety net of legal protection and trust in data stewardship. A limitation of liability would instead allow companies to plan to financially absorb information security losses rather than working to improve their internal information security practices.

Information security inadequacy in our economy among both public and private entities is rampant. Because of the nature of information vulnerability, a database that is shared by a company with trusted partners is only as secure as the lowest level of information security implemented by any trusted partner in possession of that database. Therefore, it is essential that the highest possible floor of information security be created across various entities in the economy. Further, any federal limitation of liability for unreasonable information security conduct would actively damage the attempts of regulatory agencies such as the Securities and Exchange Commission to force companies to engage in significant improvements in information security.[6]

I urge Congress to encourage better disclosure in information security conduct, however, I also urge Congress to avoid prematurely limiting the negative legal incentives for corporate self-improvement in information security conduct. The best course of action with respect to any consideration of limitation of liability is one exercising deference to federalism concerns and states' regulatory interests in redressing the harms of their citizens for information security harms. Determining the best legal regime for addressing information security breach liability still requires extensive experimentation on the state level to arrive at an optimal framework. Different states engage with consumer protection questions in different ways, and no national consensus currently exists with respect to the best course of action for information security liability. The field of information security law is very young, and best practices of conduct continue to evolve rapidly. Similarly, legal scholarship offering guidance is still scarce. Information security experts are only beginning to create a community and professionalize. A broader social and scholarly conversation on information security policy is desperately needed, and it requires time to develop. At this juncture I believe strongly that it is dramatically premature and undesirable to federally limit liability for information security misconduct demonstrating a lack of due care. A centralized disclosure system and deference to federalism concerns present the best course of action at present.

[6] In October 2011 the Securities and Exchange Commission introduced guidance which required public companies to assess and disclose material breaches of information security. To date the Securities and Exchange Commission has expressed displeasure with the level of corporate disclosure happening in connection with this guidance.

Mr. TERRY. We will. I appreciate you submitting that.
Professor Thaw, you are recognized for 5 minutes.

STATEMENT OF DAVID THAW

Mr. THAW. Thank you, Mr. Chairman.

Chairman Terry, Ranking Member Schakowsky, distinguished members of the subcommittee, I am David Thaw, Visiting Assistant Professor of Law at the University of Connecticut and Fellow of the Information Society Project at Yale Law School. I appreciate the opportunity to testify regarding the important issues of data security and consumer protection, a subject that I have spent the better part of a decade researching and working on professionally.

Federal data breach notification is important but it must be implemented properly. In my oral testimony today, I wish to address two core issues relevant to proper implementation. First, whether to address breach notification separate from broader information security regulation, and second, what burden of proof should be required if a risk-of-harm threshold is adopted for breach notification.

I understand the subcommittee to be taking up the issue of data security beginning with the question of breach notification separate from comprehensive information security regulation. I caution against this approach for two reasons. First, comprehensive information security combined with breach notification is substantially more effective than is either regime alone. As part of my research on information security regulation, I compared the efficacy of these two regimes. Specifically of note to the subcommittee's agenda, the combination of the two was nearly four times more effective at preventing incidents than was breach notification alone. I analogize the effects of breach notification alone to locking the bank or vault door while leaving a back window wide open.

Second, approaching the issue of breach notification separately requires establishing certain information categories. For example, defining what information to protect is essential to breach notification. This definition, however, has a different purpose when considering comprehensive information security. Furthermore, once established, these definitions will be difficult to change. The burden to business, for example, to reclassify information for compliance with multiple definitions is substantial.

To be specific, the types of information that should trigger notification differ from the types of information that should be protected overall. For example, medical records, wills, personal diaries, sensitive or private photographs and other similar information are all items federal law currently recognizes as sensitive personal information. State law has more narrow definitions including Social Security numbers, financial account number, and government ID numbers. Consumers should be informed about unauthorized disclosure of all this information. By contrast, sensitive information about trade secrets, computer infrastructure or security measures it not the province of the general consumer, yet such information must also be secured. On these bases, I strongly recommend that the subcommittee address breach notification and comprehensive data security concurrently.

The second issue I wish to address is the risk-of-harm threshold. Certain formulations of this threshold negatively impact informa-

tion security. Specifically, a threshold employing a negative presumption of notification, which requires proving risk of harm before triggering notification requirements, disincentivizes organizations from conducting thorough investigations. Organizations have incentives to limit investigations that might increase their liability. For example, when conducting comprehensive information security assessments, auditing and consulting firms often work together with law firms so that the results will be privileged and thus not discoverable in future civil litigation or regulatory investigations. Clients do not want to incur liability for failure to remediate security vulnerabilities identified in the assessment. A similar analysis applies to breach investigations. My research data supports this conclusion as does my professional experience. Thus, I strongly recommend that if a risk-of-harm threshold is adopted, the committee adopt an affirmative presumption of notification where risk of harm must be disproved before notification is exempted. To place the burden otherwise disincentivizes information security investigations, one of the most important tools in protecting consumers against future breaches and securing the overall information security ecosystem.

I am happy to offer any assistance to the committee as it moves forward in his work. I again thank the chairman and the ranking member for the privilege and opportunity to testify here today, and I am pleased to answer any of your questions.

[The prepared statement of Mr. Thaw follows:]

Executive Summary of Written Testimony of Dr. David B. Thaw
Submitted to the U.S. House of Representatives
Committee on Energy and Commerce – Subcommittee on Commerce, Manufacturing, and Trade

July 18, 2013: Hearing on "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?"

In this written testimony, I provide detailed information on two core issues relevant to my understanding of the Subcommittee's current agenda on data security:

I. whether to address consumer security breach notification as an initial matter, separate from and before moving to address broader information security regulation of custodians of consumer data; and

II. in the event a "risk of harm" threshold is adopted for consumer security breach notification, what burden of proof should be required to trigger notification requirements.

My recommendations are as follows:

1. that the Subcommittee consider consumer breach notification *concurrently with* comprehensive information security regulations; and

2. that if a risk-of-harm threshold is adopted for consumer breach notification, an *affirmative* presumption of notification be implemented.

The first recommendation is based on my research on the efficacy of breach notification and comprehensive information security regulation, which reveals that the *combination of both regimes is as much as four times more effective than is breach notification alone*. It also considers the risks of "definitional lock-in" whereby statutory or regulatory definitions may be adopted for one purpose (consumer breach notification) that are not well suited, or later easily adopted by entities, to other purposes such as comprehensive information security regulation.

The second recommendation is based on the risk that adopting a *negative* presumption for notification can disincentivize thorough information security investigations, which are one of the most important tools in protecting consumers against future data breaches and securing existing information systems.

Finally, I also offer a preliminary proposal for an alternate notification regime, as well as a general suggestion that a single consumer protection regulator should not have *sole* responsibility for all regulated entities, specifically including those operating critical infrastructure.

Written Testimony of
Dr. David B. Thaw
Visiting Assistant Professor of Law, University of Connecticut
Affiliated Fellow, Yale Law School Information Society Project

Submitted to the U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

July 18, 2013

Hearing on "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?"

Members of the Subcommittee:

Thank you for the opportunity to testify before the Subcommittee on the important issues of data security and consumer protection. In this written testimony, I provide detailed information on two core issues relevant to my understanding of the Subcommittee's current agenda on data security:

I. whether to address consumer security breach notification as an initial matter, separate from and before moving to address broader information security regulation of custodians of consumer data; and

II. in the event a "risk of harm" threshold is adopted for consumer security breach notification, what burden of proof should be required to trigger notification requirements.

I. Addressing Breach Notification Separate from Comprehensive Information security Regulation

I understand the Subcommittee intends to address the issue of breach notification first and separate from the issue of comprehensive information security regulation. I caution against this approach for two reasons:

1. Comparative Efficacy: breach notification alone is *substantially less effective* at preventing reportable security breach incidents than is the combination of breach notification and comprehensive information security regulation; and

2. Definitional Lock-In: adopting standards for breach notification in the absence of comprehensive information security regulation will create "definitional lock-in" for categories defined to serve the purpose of breach notification but not well suited for later adoption to broader, comprehensive information security regulation

Comparative Efficacy

My research into the efficacy of existing information security regulations,[1] specifically including the breach notification statutes present in most U.S. jurisdictions, compared the effectiveness of breach notification statutes and comprehensive information security regimes. I combined qualitative, semi-structured interviews of Chief Information Security Officers (CISO) at key U.S. organizations with quantitative analysis of data breach incidence from 2000 through 2010. The results first describe the effects of each regime at driving information security practices within organizations, based primarily on the CISO interviews.

Of particular note to the Subcommittee, the interviewees reported that a primary effect of breach notification laws was to focus intensive effort on encryption of portable devices and media containing personal information.[2] While effective at reducing the number of reportable breaches, some respondents reported that this resulted in focusing *too* much on only one area of security[3] – effectively leaving other venues available for attack. These attacks affect not only potential compromise of personal information as defined in existing breach notification statutes, but also the ability of outside attackers to compromise the integrity of critical infrastructure systems.

Such attacks are not hypothetical – in 1983, for example, a hacker group compromised the security of Memorial Sloan-Kettering Cancer Center in New York and gained access that effectively would have allowed them to alter the radiation treatment protocols of patients.[4] This compromise led to the addition in 1986 of a felony enhancement to the Computer Fraud and Abuse Act for damaging computer systems relating to medical care.[5]

As noted by the CISOs I interviewed from the healthcare sector, breach notification statutes forced them to focus increased resources on encryption – without receiving additional resources to maintain existing programs. The resultant reallocation of security budgets directed resources

---

[1] *See generally* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. (forthcoming 2014), http://ssrn.com/abstract=2241838.
[2] *Id.* at 29-30, 61-64.
[3] *Id.*
[4] *See* S. Rep. 99-432 (1986), at *2-3, 12.
[5] *See id.*, *see also* 18 U.S.C. §§ 1030(a)(5), (c)(4)(A)(i)(II).

away from where those CISOs believed they were needed most.[6] I describe this phenomenon as "Locking the Bank or Vault Door and Leaving the Back Window Open."[7] The key takeaway for the Subcommittee on this point is that focusing *solely* on consumer breach notification may have detrimental effects to other, critical areas of information security.

My quantitative research also presents information of substantial import to the Subcommittee's work. By analyzing periodic breach incidence data from January 1, 2000 through December 31, 2010, I determined that the combination of consumer breach notification and comprehensive information security regulation was as much as four times more effective at preventing reportable breaches of consumers' personal information than was breach notification alone.[8]

Definitional Lock-In

Approaching the issue of breach notification separately will generate an effect I describe as "definitional lock-in" – key definitions in regulations will be determined at an early stage, based on limited scope of purpose not well-suited the broader purposes later envisioned. Specifically, key definitions such as the subject of information to be protected (often referred to as "Personal Information") will be defined for the purposes of consumer breach notification; purposes that are very different than those appropriate to comprehensive information security regulation. Lock-in occurs as a result of the substantial cost to organizations of later "re-classifying" information based on additional categories established by new regulation. This process, when applied to existing data,[9] is often cost-prohibitive and may raise regulatory burdens too high for effective compliance, thus pressuring legislators and regulators to retain existing definitions.

To be specific, consider the example of the types of information that should be subject to protection. In the case of breach notification, this information is most commonly referred to as "personal information" or "personally identifiable information." These terms have widely varying definitions. At the state level, a least common denominator exists: the combinations of an identifying item, most commonly an individual's name, with one of three categories of more sensitive information:

- the individual's Social Security Number;
- the individual's financial account numbers, along with any identification code necessary to access the account; or

[6] Thaw, *supra* note 1, at 63.
[7] *Id.* at 61.
[8] *Id.* at 58.
[9] as differentiated from new data generated as technology advances

- the individual's government-issued identification number (usually driver's license or state ID)

The stated purpose of most jurisdictions' breach notification statutes is to enable consumers to take steps to protect themselves by requiring custodians of this information to inform consumers when those custodians have lost control of this information.[10] Yet many other types of information may pose a great harm to consumers. For example:

- medical records
- wills
- diaries
- private correspondence (including e-mail)
- financial records
- photographs of a sensitive or private nature; [and]
- similar information

are all categories of information federal criminal law considers sufficient to warrant substantial criminal sentence enhancements for individuals convicted of computer crimes involving identity theft.[11] The Department of Health and Human Services,[12] the Department of the Treasury,[13] and the Federal Trade Commission[14] each have offered additional definitions of information they consider to be "sensitive" to consumers. All of this information should be the subject of consumer protection. Additionally, consumers should be informed whenever this information is subject to unauthorized disclosure as is necessary to take steps to protect themselves.

These categories are hardly comprehensive of the types of information that need to be protected by comprehensive information security regulations. Corporate trade secrets, including sensitive data about products not yet available outside the United States, sensitive business development plans, information about critical infrastructure systems such as water, electric, or telecommunications grids, and information security plans are all sensitive information that are

---

[10] *See, e.g.,* CAL. BILL. ANALYSIS, S.B. 1386, Cal. Assembly, 2001-2002 Reg. Sess. (Aug. 23, 2002) (Senate Third Reading, analysis of Saskia Kim).
[11] *See* UNITED STATES SENTENCING GUIDELINES MANUAL § 2B1.1(b)(16), *see also* § 2B1.1 Application Notes.
[12] *See* 45 C.F.R. § 160.103, definition of "individually identifiable health information."
[13] *See* 12 C.F.R. Part 30, App. B, § (I)(C)(2)(b) ("Consumer information means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the bank for a business purpose. Consumer information also means a compilation of such records. The term does not include any record that does not identify an individual.")
[14] *See generally* Protecting Personal Information: A Guide for Business, FEDERAL TRADE COMM'N at 5, *available at* http://www.business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf (suggesting a broad definition of personal information that includes "other sensitive information").

not the province of the general consumer. Yet a failure to secure this information may have costly effects, and not just to the organization experiencing the breach. If a business partner of a new pharmaceutical fails to properly secure their information systems, or the information technology services provider to a major financial institution or exchange fails to implement appropriate controls on administrative accounts, substantial negative effects to the broad economy may result if those systems are compromised. None of these eventualities necessarily involves consumer information, but each clearly demonstrates a public interest in collective security.

If a definition of information to be protected is developed based solely on consumer breach notification, the downstream information security implications will be costly. Either organizations must engage in expensive reclassification of information and redesign of their information security programs when new regulations are subsequently implemented, or large areas of information may be left vulnerable if the regulations fail to expand the definition of information to be protected. In either case, the cost of considering breach notification separate from comprehensive information security measures would be high.

In summary, on these bases – the decreased efficacy, misallocation of resources, and risks of definitional lock-in – I strongly urge the Subcommittee to address consumer breach notification and comprehensive information security concurrently.

II. Considerations if a "Risk-of-Harm" Threshold is Adopted for Breach Notification

When considering the issue of consumer breach notification, legislators and regulators frequently confront the issue of *when* to require notification. Among existing law, some jurisdictions require notification in all cases of loss-of-control (subject to the "encryption exception"[15]) whereas others adopt what is known as a "risk-of-harm" threshold. This Section of my testimony takes no position as to which approach is preferable – the empirical data on this result remains mixed. (In Section III, I introduce a preliminary proposal for an alternate regime.)

Rather, the focus of this Section addresses the *information security implications* of certain formulations of the risk-of-harm threshold. Specifically, I note to the committee that some formulations negatively impact information security procedures and outcomes.

[15] To the best of my knowledge, no current U.S. jurisdiction, inclusive of (unclassified) federal regulations, *requires* notification to *consumers* in the event of loss of control of unencrypted and otherwise unsecured personal information subject to notification requirements under applicable law.

Risk-of-harm thresholds may have many forms, but generally can be categorized according to the *affirmative* or *negative* presumption of notification. An *affirmative* presumption of notification requires a data custodian who experiences a breach to affirmatively demonstrate that the specified risk of harm threshold *is not satisfied* before they are exempted from consumer notification requirements. A *negative* presumption of notification *does not* require a data custodian who experiences a breach to notify consumers *unless* an investigation reveals that the specified risk of harm threshold has been satisfied.

A negative presumption of notification carries substantial, worrisome implications for information security procedures and outcomes. Specifically, this presumption disincentivizes organizations from conducting thorough security investigations.

Organizations have incentives to limit the scope and scale of investigations that may uncover information potentially exposing the organization to liability. For example, when conducting comprehensive information security assessments, auditing and consulting firms often work together with law firms so that the results of these assessments will be privileged as attorney-client work product and thus not subject to discovery in civil litigation or regulatory investigations. Clients of such firms often desire to learn about the risks they face, but do not want to incur liability for failure to remediate security vulnerabilities identified in the assessment. This problem is particularly compounded when faced with low-probability/high-risk vulnerabilities for which the cost of remediation is high. While generally protected by the business judgment rule, executives of publicly-traded organizations still bear a fiduciary duty to act in the best interests of their shareholders. A risk analysis might well reveal that the probability is sufficiently low not to justify the direct costs of remediation when combined with the cost of business disruption and other indirect cost. While I do not suggest that organizations engage in willful ignorance of their legal or regulatory obligations, my research data and professional experience support the conclusion that organizations can have substantial incentive not to pursue a comprehensive investigation if it might trigger additional regulatory compliance requirements.[16] Conversely, if pursuing that investigation might alleviate the organization of regulatory compliance requirements (e.g., exempt the organization from consumer notification), my research and professional experience support the conclusion that organizations can have substantial incentive to thoroughly pursue that investigation.

Thus I strongly recommend that, if the Subcommittee considers use of a risk-of-harm threshold, that it adopt an *affirmative* presumption of notification. This will avoid disincentivizing thorough information security investigations, which are one of the most important tools in protecting consumers against future data breaches and securing existing information systems.

[16] *See generally* Thaw, *supra* note 1.

III. Preliminary Proposal for a Bifurcated Notification Regime

As noted in Section II above, for the reasons therein, I take no position as to whether a strict loss-of-control or a risk-of-harm threshold is preferable from an information security perspective. In this final Section, I briefly introduce an alternate notification regime I am currently developing. This proposal builds on similar regimes found in states such as New York,[17] Massachusetts,[18] and Virginia,[19] each of which require notification to central state regulatory authorities in addition to notification to consumers in the event of a reportable data breach.

Under such a bifurcated notification regime, organizations experiencing a loss-of-control of any covered data would be required to report that incident to a centralized reporting authority, most likely a federal regulator such as the Federal Trade Commission. Consumer reporting would be triggered in certain cases deemed appropriate to where consumers can take steps to protect themselves and/or when consumers have an interest in awareness that their sensitive information was subject to unauthorized disclosure.

This bifurcated notification regime, if properly implemented, could achieve many of the goals of consumer breach notification while mitigating the risks of "over-notification" often raised by critics of strict loss-of-control regimes.[20] Specifically, consumers would receive appropriate notification, while all incidents would nonetheless be reported. Thorough information security investigations would be a requirement under this regime as part of the centralized reporting requirement. Additionally, the regulatory agency receiving the reports would have the ability to follow-up in cases where they suspect consumer notification should have occurred but did not, to follow-up if there is evidence a broader pattern of information security deficiencies may be present, or to follow-up and provide support if it believes the organization requires additional information security and/or law enforcement support.

I stress in my testimony that this proposal is *preliminary*, and I lay out the basic characteristics as guidelines. I encourage the Subcommittee to investigate this proposal – similar versions of which currently are in place in some U.S. jurisdictions, as noted above – to determine what benefits it may afford at the Federal level.

---

[17] *See generally* N.Y. GEN. BUS. LAW § 899-aa.
[18] *See generally* MASS. GEN. LAWS ch. 93H-1 et seq.
[19] *See generally* VA. CODE ANN. § 18.2-186.6.
[20] This is not to suggest I believe over-notification currently is or is not a problem. Rather, I only suggest that if over-notification is of concern to the Subcommittee, a bifurcated notification regime can address such concerns.

IV. Comments Regarding the Issue of a Unified Regulatory Regime for Information Security

Although I do not understand the Subcommittee's core agenda for this Hearing to include the question of whether information security provisions should be unified under a central regulator, this question is inextricably intertwined into the issue of breach notification.

Information security, also known as "cybersecurity,"[21] is a layered exercise. I recently discussed this phenomenon in greater detail,[22] describing that its challenge is the protection or regulation of four different categories of information systems:

- military and defense operations
- non-military government information systems
- private sector critical infrastructure, and
- non-critical private sector information systems

The competencies required to address threats faced within each of these categories differ in several ways. Military and defense operations, for example, must adopt a more stringent "risk prevention" approach, which they also are better suited to achieve because of the command-hierarchy backed by the threat of criminal punishment inherent in the military.

Private companies operating non-critical information systems, by contrast, have a fiduciary duty to their shareholders to apply the most efficient level of protection – which may differ widely from the "strongest" level of protection. They also lack the ability to enforce as rigid a hierarchy as the military.

Private companies operating critical infrastructure, such as utilities, telecommunications, financial systems, and healthcare systems, bear many of the same characteristics of other private

---

[21] As noted by Professor Andrea Matwyshyn, "referring to all of information security, particularly in private sector contexts, as 'cybersecurity' is technically incorrect." Matwyshyn describes this misnomer as ignoring the aspects of physical security inherent in "holistic" protection of data maintained by an enterprise. I concur with this assessment, and further suggest, as consistent with the Administrative/Technical/Physical breakdown described in Part II, Section B of Thaw, *supra* note 1, that such a characterization also overlooks the administrative aspects involved in protecting and security information. *See* Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, NW. L. REV. at 36, n. 105 (forthcoming 2013) (cited with permission of author); *see also* David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 101, 122, 137 (2013), http://ssrn.com/abstract=2226176 (discussing the distinction between purely-technical restrictions on computer usage and comprehensive administrative, technical, and physical restrictions thereon).

[22] *See* David Thaw, *A Flexible Approach to Cybersecurity Regulation*, REGBLOG (July 9, 2013), https://www.law.upenn.edu/blogs/regblog/2013/07/09-thaw-cybersecurity.html.

organizations, but they possess a heightened protection obligation stemming from the substantial negative externalities if their systems fail or are compromised.

This categorization suggests two conclusions the Subcommittee may wish to consider should the subject of single vs. multiple federal regulators arise in its work:

1. Even within industrial sectors, organizations are often substantially heterogeneous with respect to their information security competencies and vulnerabilities. Thus flexibility within regulation, which may be accomplished by delegation of certain rulemaking authority to administrative agencies, is essential.

2. Entities at "higher" tiers of criticality should not be regulated *solely* by regulators at lower tiers. For example, a critical infrastructure provider should not be regulated *solely* by the Federal Trade Commission, whose core competency is protecting consumer information, and must *at least* be regulated by the Federal Communications Commission, whose core competency is understanding the heightened protection obligations that may face providers of critical infrastructure.

Conclusion

In closing, I wish to reiterate my primary recommendations to the Subcommittee:

1. that the Subcommittee consider consumer breach notification *concurrently with* comprehensive information security regulations; and

2. that if a risk-of-harm threshold is adopted for consumer breach notification, an *affirmative* presumption of notification be implemented.

I again thank the Chairman, the Ranking Member, and the Members of the Subcommittee for the opportunity to testify on this important issue. I would be pleased to provide any follow-up information the Subcommittee may find helpful as it proceeds with its work on this topic.

Respectfully submitted,

David B. Thaw, J.D., Ph.D.

Visiting Assistant Professor of Law, University of Connecticut
Affiliated Fellow, Information Society Project, Yale Law School

Mr. TERRY. Thank you very much for your testimony and appreciate the two law school professors here. It makes me feel—I had flashbacks to law school during your testimony.

With that, I will start the questions—the answer to this is just yes or no. It was clearly clear in some of the testimonies but I do want to get it succinctly on the record starting with Mr. Richards and then going down to Professor Thaw.

Do you believe there should be a federal notification law? Mr. Richards?

Mr. RICHARDS. Yes, we do, Mr. Chairman.

Mr. LIUTIKAS. Yes, we do, Mr. Chairman.

Mr. GREENE. Yes, sir.

Ms. MATTIES. Yes.

Mr. TERRY. Now we get to the murkier.

Ms. MATWYSHYN. Exactly. Yes, provided the standard is at the highest level and does not preempt State law, as well as conduct being carved out to allow for States to experiment.

Mr. THAW. Yes, provided implemented properly. I provide detail in my written testimony on this, and concur with Professor Matwyshyn's statement.

Mr. TERRY. See, that is the flashbacks. There is always enough room to screw up on the test now.

Ms. MATWYSHYN. It always depends, right?

Mr. TERRY. It always depends.

And the reason why I think it was important to just lay that item of foundation is that with 48 States and territories combined already having at least at the multinational level, you have a level of sophistication where they are already in compliance and then there is a level of concern that a new national standard just creates 49 instead of 48. So that brings us to what Professor Matwyshyn said in her "but", and that is no State preemption. So how does it work without preemption, and who wants to start? I will go with Dr. Matwyshyn first and then anyone else that wants to speak on preemption.

Ms. MATWYSHYN. So I actually consulted with a California government official responsible for enforcement, and provided that the framework on the national level provides a comprehensive disclosure regime and States and their enforcement agencies have direct access to this information as well as consumers, everyone wins because the information would simply be centralized. So if the disclosure requirements adequately conceptualize the questions that consumers and enforcers want to know, States, I believe, would be happy with a centralized regime and there wouldn't be a problem with enforcement, however, because of limitations of resources on the part of the Federal Trade Commission I believe should remain on the State level.

Mr. TERRY. All right. Mr. Richards, Liutikas and Greene, and Ms. Matties, quickly, though.

Mr. RICHARDS. Sure. Well, we believe the patchwork framework occurring in State laws are very duplicative in some cases, and in a lot of cases don't make sense. North Dakota, for example, requires notice of a breach of name and birth date so there are different qualifications in terms of PII and what information you should focus on. New York requires notice of security breaches

made to three separate State agencies. I think federal preemption is important but I don't think you should undermine strong consumer protections that are currently held and enjoyed at the State level.

Mr. TERRY. Thank you. Mr. Liutikas?

Mr. LIUTIKAS. I mean, at the end of the day I think we believe that first and foremost that consumers need the notification standard but in providing that standard, we could also simplify matters substantially for the small- to medium-sized business which the current technology infrastructure allows them to operate in a way that is much bigger than maybe they could have done some years ago. So I think centralizing that notification standard and avoiding having the issue of determining whether or not a variety of State laws applies or does not apply would be extremely beneficial to the small- to midsized business that simply doesn't have the resources.

Mr. TERRY. Interesting. Mr. Greene?

Mr. GREENE. I would echo what Mr. Richards said, that if you have essentially 49 standards, you are just creating another box you have to check to ensure that you are doing everything right. If you do have a breach, you are not going to speed the process of understanding the scope of your breach of who you need to notify.

Mr. TERRY. Thank you. And Ms. Matties, I am actually going to change the question for you to more personalized because of your background and experience with the FTC. There has been a suggestion that at least with some of the telecoms that the FTC has the experience on data breach and notification in those areas. If there is a national bill, should it include the telecommunications and video with the FTC?

Ms. MATTIES. Yes. The FTC has had more than 10 years of experience working on data breaches and data security cases, so they are well equipped to handle these kinds of cases. And I just would like to point out that there is already a model in Do Not Call for consolidating experiments in the States with consumer protection. A number of States have consumer protection laws for Do Not Call in individual States, and when the national standard became applicable, it really made things a lot easier for both businesses and for consumers because now consumers have a one-stop shop to go and put their name on a list. That would be a similar aspect here.

Mr. TERRY. All right. Thank you very much.

The ranking member, Jan Schakowsky, is now recognized for 5 minutes.

Ms. SCHAKOWSKY. Thank you very much. Mr. Chairman, I just want to acknowledge that as important as this is to consumers that maybe in the future we could have a consumer witness or two to talk about some of their experiences. I think it would helpful to inform our committee.

Talking about data breaches, Professor Matwyshyn, do you foresee potential harms to the development of effective information security laws if Congress enacts certain breach notification provisions without enacting a well-considered data security law at the same time? I know Professor Thaw addressed that. And if so, what would they be?

Ms. MATWYSHYN. If I am understanding the question correctly, I believe that the optimal approach at this juncture is to bifurcate,

to divide off the questions of data breach notification harm in this Nation from the questions of the best standard for liability arising from data security breaches.

Ms. SCHAKOWSKY. To separate those two?

Ms. MATWYSHYN. To separate those two out. While the States have shown us the way and adequately experimented with notification, the questions of liability, how to craft it, what the standards are, what reasonable conduct is, that is a moving target and still very undeveloped, both from the standpoint of the information security community as a just-now-coalescing body of experts and from the standpoint of States having different approaches to consumer protection and the connection to other bodies of law. The Securities and Exchange Commission is starting to regulate in this space.

These issues are tied with broader questions of software liability generally, and if we start to regulate too early, we may disrupt existing bodies of law and stifle innovation that is responsible and consumer protection.

Ms. SCHAKOWSKY. OK. I do want to put the same question to Professor Thaw and see if the two of you are in agreement.

Mr. THAW. I agree with Professor Matwyshyn in the respect that the States have the ability to provide important experimentation. However, I am concerned about the resources that the States have on the technical side. With respect to the legal standard, I agree with Professor Matwyshyn. They can experiment and provide us with valuable data. However, this is a highly interconnected issue across the entire country, and I do not believe that the States have sufficient resources for enforcement or for simple providing the research and investigation necessary to know what standards would be effective at a national level as opposed to at a State level.

Ms. SCHAKOWSKY. Let me get into the issue of data brokers. Most consumers have never heard about data brokers but there is a several-billion-dollar industry that knows the name, address, age, purchasing habits of nearly every American consumer. One company in this industry possesses on average 1,500 data points apiece on each of 190 million individuals in the United States and a profit of more than $77 million on this information. So again, let me go to Professor Matwyshyn.

The Data Accountability and Trust Act as was passed in the 111th Congress would have required data brokers to submit their security policies to the FTC and allow the Commission to perform or mandate the performance of security audits following a breach of security. What is your opinion on these kinds of provisions regarding data brokers?

Ms. MATWYSHYN. In that case, I believe you mentioned it was following a breach?

Ms. SCHAKOWSKY. Yes.

Ms. MATWYSHYN. That would be entirely consistent with the types of proposals that we are considering now for centralized breach notification. The goal is to get as much information about breaches, how they happened, why they happened, the level of security that is in place in the particular organization to provide the information to both consumers and enforcement agencies to determine which entities are the good actors and which entities are the actors that still have a way to go to improve the level of care.

Ms. SCHAKOWSKY. With just a minute or two, actually less than that, you may also want to comment on data brokers and the role that they play and how they should be regulated, Professor Thaw?

Mr. THAW. With respect to data brokers, I draw the committee's attention to the fourth section of my written testimony where I identify different levels of criticality, and I would suggest that data brokers are at a higher level of criticality, the reason being that the information they contain, to use Professor Matwyshyn's earlier example, could be information which is an authentication credential such as your mother's maiden name or your favorite color, your first pet, something that you use to secure other data that is very sensitive. For this reason, they should be regulated at a higher level, and this is something that cannot be overlooked.

Mr. TERRY. Thank you, and now we recognize the chairman emeritus for 5 minutes.

Mr. BARTON. Thank you, Mr. Chairman. I am going to try to give you a little bit of that time back.

I think in your questions, Mr. Chairman, we established the panel does support a federal standard for notification. My question would be, does the panel also support going beyond that so that we get into the prevention and the liability issues? Does everybody, you know, support a federal law that goes beyond breach notification?

Mr. RICHARDS. I think that would depend on—we would obviously have to see the legislation but I certainly think we should probably change the culture of how our society looks at cybersecurity or information technology and how do you protect the information. Instead of making it an IT department issue, make it a CFO issue and really change the thinking and the approach to how we approach data protection in the country.

Mr. LIUTIKAS. I think we also need to look to industry associations like CompTIA which provides the industry a platform for collaborating on standards and best practices and their industry credentials such as the CompTIA Security Trust Mark credential, which audits the security practices of an organization. So I think in light of considering options such as that, I think we should also look at the options that the industry can provide as well.

Mr. GREENE. Conceptually, we support the notion of requiring security standards, so you are looking to prevent the breach, not just to mitigate after, and the same thing with the encryption. So if you have a breach, you are limiting the damage that can happen. But as Mr. Liutikas said, there are a lot of existing industry standards that are effective, and any type of standard needs to be very flexible and performance based. We don't want to be mandating anything specific in statute when we have a very shifting threat environment. So the notion of saying you need to be secure is OK, but if we get into the where we are mandating specific types of solutions, I think that could be problematic.

Ms. MATTIES. CTIA members and the broader 21st Century Privacy Coalition is interested in talking about data security for sure but we are happy to see that we are starting with data breach notifications.

Ms. MATWYSHYN. No limitations of liability are appropriate at this juncture. I think we are a little too premature. On the state

level, experimentation would be great. A negligence standard perhaps evolving would be a good move. I think we are ready to address breach notification but I would be cautious in approaching liability.

Mr. THAW. Yes, if properly implemented, and I note that respectfully, Mr. Richards, I am concerned with his proposal of making this a CFO issue. While that is appropriate to companies' fiduciary duties under state law, it is not appropriate to the question of negative externalities that would result from breaches in one organization to the overall information ecosystem. I also do concur with my panelists' opinion that flexible standards are important.

Mr. BARTON. I agree with flexible standards.

Mr. Chairman, I want to turn it back, but let me simply say, back in the 1930s when we had a rash of kidnappings, the Congress did not pass a kidnapping notification law. They passed strict laws delineating it was a federal crime if it crossed State lines and empowered the FBI to use every means possible to go after the kidnappers. We are not talking about stealing our children but we are talking about stealing our identifies, and I would hope that this subcommittee and the full committee goes beyond breach notification law, and with that, I yield back.

Mr. TERRY. It is the intent. I am going to call on Mr. Barrow, and then we will adjourn, so if you are next in line as a Republican, you can go to the meeting.

Mr. Barrow, you are now recognized for 5 minutes.

Mr. BARROW. Thank you, Mr. Chairman, and thank you for setting the table with your questions. I want to follow up some of the issues that you raised.

You know, privacy is important to me. The right to be secure in your persons and papers from State intrusion is in the Fourth Amendment. Warren and Brandeis said that the right to be let alone, the right of privacy is the right most prized by civilized men, I guess we would say today civilized men and women. I certainly agree with them on that.

I guess the general consensus is that the current regime of essentially 48 separate State and territorial jurisdictions regulating this matter and our common market of the United States just ain't working. I think we all agree with that, and there is a general need for some federal guidelines, some federal standards for a uniform law in our national economy.

Mr. Richards, Mr. Liutikas, Ms. Matties, you each talk about the subject of preemption, the need to preempt conflicting state laws. I want to ask the other members of the panel, what is the appropriate scope of federal preemption in this area? Yes, ma'am, go ahead.

Ms. MATWYSHYN. I believe the appropriate scope if creating a harmonized disclosure form but enforcement should be shared in the same way that it is in securities regulation. In the securities regulation context, we have multiple sources of oversight—the FCC, state level, securities regulators, other agencies inside the States.

Mr. BARROW. Are you proposing a uniform law but shared responsibility with respect to enforcing the same law so the federal regulator would set the rules and regulations but the State folks

might enforce the same federal law if the federal government isn't devoting enough resources to enforcing its law, the national standard? Is that what you have in mind?

Ms. MATWYSHYN. In the same way that securities disclosures happen on the federal level primarily but a particular state may have requirements in terms of protecting its citizens.

Mr. BARROW. Well, additional requirements, additional substantive regulations and obligations and duties are different from a uniform standard that either the federal prosecutor or the state prosecutor can enforce the same law—one land, one law. That is a very different matter. And having the right at the state level to enforce a federal standard is different than being able to make your own standard and enforce that in addition to the federal standard, so I want to talk about whether or not there are other folks on the panel who agree with the proposition that federal regulation ought to occupy the field when it comes to the substantive obligations and responsibilities in this area. Mr. Greene?

Mr. GREENE. Sir, we would agree that it should occupy the field but ultimately I think the notion of state enforcement would be acceptable as long as we are talking about a uniform federal standard.

Mr. BARROW. I got you.

Professor Thaw?

Mr. THAW. State enforcement concurrent with federal enforcement would be appropriate, and I want to emphasize that in either case, centralized notification and collection by a federal regulator so that we have information on what is going on is critical.

Mr. BARROW. All right. We have had a slight diversity of opinion with respect to who ought to be able to make the rules, but there seems to be a general consensus that as long as we are enforcing the same rules, it doesn't matter which government the cop reports to if they are enforcing the law.

I want to get to the subject of who ought to be the federal regulator. I think, Ms. Matties, you said that we not only need to have a uniform federal system but it ought to be headed up by the FTC as opposed to, say, the FCC. Does anybody disagree with that on the panel as to which federal regulator ought to be making the rules that we will be trying to enforce on a consistent basis nationwide? Does anybody disagree with that approach? Professor Thaw?

Mr. THAW. I agree that the Federal Trade Commission is the most appropriate for consumer regulation. However, that should not exempt critical infrastructure providers, which would include telecommunications providers from regulations to which they would also be subject by their regulators. Those regulators, for example, the Federal Communications Commission, the Nuclear Regulatory Commission are better familiar with what are the challenges faced by their entities, and if they need to impose additional standards, they should not be prevented from doing so by consumer regulation.

Mr. BARROW. Is it your position that they can regulate in their areas of subject-matter jurisdiction and should not be able to regulate in the area of consumer protection?

Mr. THAW. If I understand your question correctly, my position is not that they should be pushing out the consumer regulator so

the consumer regulator has no authority but only that they may and if necessary should regulate concurrently with the consumer regulator.

Mr. BARROW. What do other members of the panel feel about that? Mr. Richards, Mr. Liutikas, Mr. Greene?

Mr. RICHARDS. Mr. Barrow, I would say that the FTC definitely when it comes to consumer information certainly I think our approach to privacy in this country is somewhat patchwork when you are dealing with HIPAA and the Fair Credit Reporting and Gramm-Leach-Bliley, so I certainly think that the current functional regulators also have a good system in place but the FTC certainly is equipped when it comes to consumer information.

Mr. BARROW. Mr. Liutikas?

Mr. LIUTIKAS. I would generally concur with that although I think we would have to conduct some further analysis and see what really makes sense at the end of the day. You know, the question right now is somewhat theoretical but I think overall makes sense, and we certainly support having a federal agent, so whichever department that is.

Mr. BARROW. Well, my time has run out, Mr. Greene. I regret that. But if any of you all want to follow up on this and supplement the responses that you have given or that others have given on this subject, please feel free to do so for the record.

Thank you so much, and thank you, Mr. Chairman.

Mr. TERRY. And I mistakenly used the word "adjourn" earlier. We are recessing until probably 1 o'clock, hopefully by 1:03 or 1:04 we are asking questions of you. So thank you for your patience, and we will see you in 50, 55 minutes.

[Recess.]

Mr. TERRY. I appreciate you all being back. We are missing Professor Thaw for the moment.

Ms. MATWYSHYN. He went to go fetch a deserted bag so that they don't confiscate it. He will be right back.

Mr. TERRY. Oh, that is important. We will string things out, but we will start with the questions. We have a short time before either votes or the next committee takes over. So we don't want to delay until he comes back but we will start with other people.

Vice Chairman of the subcommittee, you are recognized for 5 minutes, Mr. Lance.

Mr. LANCE. Thank you, Mr. Chairman, and good afternoon to the panel.

To Ms. Matties, what, in your opinion, should be the proper standard for breach notification? Suspicion that a breach has occurred or actual evidence that such a breach has occurred?

Ms. MATTIES. Actual evidence that a breach has occurred.

Mr. LANCE. So you would have a higher standard before——

Ms. MATTIES. Yes.

Mr. LANCE. Thank you. And number two, should a breach have to result in identity theft or other financial harm to require consumer notification?

Ms. MATTIES. There certainly should be consumer notification for identify theft and financial harm, and we are willing to talk to you about the other kinds of harms that might result from a breach of other information.

Mr. LANCE. Do you have suggestions regarding that other than financial harm?

Ms. MATTIES. We are still working with our members to talk about this, and we look forward to talking to you as well about it.

Mr. LANCE. Thank you.

Are there others on the panel who have an opinion on that? Yes, Professor.

Ms. MATWYSHYN. I believe that actual harm should not be required for notification. It serves a function to advise consumers of the occurrence of a breach and also to allow for tabulation and centralization of information about security practices so that we can collectively get a better picture of the entirety of the economy and the behaviors that are happening around information security.

Mr. LANCE. Thank you.

Others on the panel? Mr. Richards?

Mr. RICHARDS. I thank you. We would—our standard would be that there should be a notification requirement if the breach presents a significant risk of harm to consumers and may perpetuate identity theft.

Mr. LANCE. A significant harm to consumers, which might be a slightly different standard from financial harm, if I am understanding you accurately?

Mr. RICHARDS. Yes.

Mr. LANCE. Professor Thaw?

Mr. THAW. I believe that notification should at least occur in all cases to a central reporting authority, which could be a federal regulator, that a substantial risk of harm is too high a threshold. I base this on the civil litigation where it was virtually impossible for any case to advance based on those types of claims, and with respect to the types of harm, I believe this requires further investigation but should not be limited to identity theft.

Mr. LANCE. And if the notification were made to an entity of the federal government, that entity would then in turn determine whether further notification should be made to the consumer?

Mr. THAW. That would be conditional on whether or not notification had already been made also by the company. I think at least the agency should retain the right to make that determination.

Mr. LANCE. Thank you. Are there other thoughts from the panel? Hearing none, Mr. Chairman, I am finished with 2 minutes to.

Mr. TERRY. Thank you, Mr. Lance.

Mr. Harper, you are now recognized for 5 minutes.

Mr. HARPER. Thank you, Mr. Chairman, and thank each of you for being here, and it is a very important issue to each of you, I know, and certainly it is to our country and many businesses, and I will start with you, if I could, Mr. Richards, and ask you, how would you define a breach that constitutes a reasonable risk of harm to consumers?

Mr. RICHARDS. Sure. Thank you, Congressman. In terms of a reasonable risk, we believe that data that could be used to perpetuate identity theft, if you were to allow someone to use, log in to or access an individual's account or establish a new account using that individual's identifying information, and we would hold it to that standard.

Mr. HARPER. So as you define a breach, how do you define a significant risk of harm to consumers?

Mr. RICHARDS. If there is a risk of identity theft or stealing personal information and using or creating a new identity based on that personal information.

Mr. HARPER. Well, how should we or how would we define what constitutes a significant risk of harm to consumers? If you were advising us, if Congress did define the type of personally identifiable information that constitutes harm to consumers, is it possible that such a list would keep up with technological innovations?

Mr. RICHARDS. Yes, sir. I think it is important not to mandate specific technologies. As you know, we need a flexible framework. Some technologies today and best practices can render data useless, and in that case, if a company or an organization is trying to take the right approach and render the data useless, we believe a safe harbor should be granted to incentivize that good behavior if the information is indecipherable, but we need a flexible framework in an effort not to undermine innovation for new technologies that come down the line.

Mr. HARPER. And I know I am going to mispronounce your name, Ms. Matties, if I could ask you a question. My understanding from your testimony is that different data breach requirements apply to different entities, even for the same information. Is there any public policy justification for applying different data breach requirements to the same information?

Ms. MATTIES. No, there is not.

Mr. HARPER. And I will ask this panel-wide, if I could. All of your testimony points out that States have different notification requirements and definitions. Is there a certain time frame post breach that you believe individuals have a right to be notified? I would like to hear each of your responses on that, and I will start with you, Mr. Richards.

Mr. RICHARDS. Certainly. Well, we think there needs to be a little bit of time in order for a company to perform cyber forensics. We don't have a specific position on a specific time frame but our businesses and their approach is as quickly as possible and consulting with law enforcement and others, and we follow up on our due diligence and report it to the consumer as quickly as possible.

Mr. HARPER. Well, following up on that, how can—maybe you can walk me through. How is notification without unreasonable delay how that really works in the real world?

Mr. RICHARDS. Well, I think in terms of, if you look at the different State requirements, there is different time frames that are offered. Puerto Rico is 10 days to notify folks. Vermont is about 14 days. Minnesota requires reporting to credit bureaus within 48 hours. So sometimes when you are looking at the condensed time frame, you are really trying to figure out the extent of the breach, what has been breached. So I think in terms of those time frames, it is a very short turnaround and a very short fuse, and I think companies want to make sure that they have the right answers before they disclose information publicly but I believe they do have the responsibility to report it to consumers.

Mr. HARPER. Thank you. And I will ask each of you, is there a certain time frame post breach that you believe individuals have a right to be notified?

Mr. LIUTIKAS. Yes, Congressman, we certainly—and we will mirror a little bit of what Mr. Richards said. We believe in a reasonable time frame in which to notify. I think it is just important for the exceptions to be made for instances where law enforcement needs to act or other information needs to be gathered so that the correct information is being provided to the consumers. So we don't have an exact timeline that we recommend but we do recommend having exceptions for those legitimate reasons.

Mr. HARPER. And Mr. Greene, I think I can at least get your response before my time is up.

Mr. GREENE. Sure. I would say that you definitely need to have enough time so the company can determine the scope of what was lost and what wasn't lost, fix the vulnerability. You don't want to go public and basically hang a target around your neck, and I would say, though, a rush to report can be bad. Every incident is different. I think if there is one rule, it is that first reports are pretty much always wrong. With respect to the breach about Congress today, you are going to see what was published today a week from now is going to be outdated, is going to be different, so you need to allow time. It needs to be as quickly as possible but you need to make sure that you are getting it right. It is better to be right in most cases than it is to be fast.

Mr. HARPER. Thank you, and I believe my time has expired so I yield back, Mr. Chairman.

Mr. TERRY. Thank you, and now the chair recognizes the gentleman from Texas, of which he is very proud and will probably mention that. He is recognized for 5 minutes.

Mr. OLSON. Thank you, Mr. Chairman, for holding this hearing, and thank you to the witnesses for attending.

Mr. Chairman, you should know that I got my plug in with all the witnesses as to why they should move to the great State of Texas before we were gaveled in at 11 o'clock, so we are done with that business.

At the end of the day, this hearing, to me, is about two questions. Number one, is federal legislation necessary when data has been breached. If the answer is yes, then what should that legislation look like. In your written testimonies that I reviewed last night, it appears that federal legislation would help protect consumers, but Mr. Richards raises the point that there are some technology companies it is helpful but not vital. The two professors were concerned with, you know, federal government overreach and taking over what the States are doing pretty well. But I believe this difference raises an important point, that if we pursue legislation, we must carefully draft it to ensure that the federal government doesn't become the 49th entity out there that companies must comply with. We should have a Hippocratic oath for data breaches: harm has been done; do no more harm.

In regards to the ultimate decision to pursue legislation, consumers expect their privacy of their personal information to be protected, and I know you all agree we must keep them at the forefront of this conversation and debate.

My first question is for you, Ms. Matties. Do you think the existence of 48 different data breach regimes results in brief notifications being faster or slower?

Ms. MATTIES. I think it makes it slower. Companies try very hard to comply with all the laws out there but it certainly is a distraction, at best, from the other tasks that they need to complete when dealing with a data breach as has been discussed by the other panelists.

Mr. OLSON. Does anybody else care to comment on that, faster or slower? Professor Thaw?

Mr. LIUTIKAS. Congressman, I think it makes it significantly—oh, I apologize.

Mr. OLSON. You are up next, Mr. Liutikas.

Mr. THAW. I believe historically it has made it slower but it absolutely does not need to. It is a very formulaic regime for which procedures can be developed, for example, to analogize to something with which I believe many people may be familiar, Legal Zoom, the product that provides—you punch in the information, we generate a will or something similar. I could develop today a program that would handle the current jurisdiction requirements in place.

Mr. OLSON. OK, Mr. Liutikas, come on in.

Mr. LIUTIKAS. Thank you, Congressman. In addition to making the process slower today, I think the process of actually evaluating all of the different requirements and the laws out there also creates more opportunity for not properly reporting under a variety of State laws. So not only does it slow it down, I think there is more opportunity for mistakes to be made as well.

Mr. OLSON. Thank you.

Another one for you, Ms. Matties. How do wireless companies deal with the fact that States have different definitions of personal information? Can that result in over-reporting in some States? Does it create consumer confusion? And what harm may companies incur if they over-report and some examples? So basically over-reporting, confusion, harm, examples.

Ms. MATTIES. I am not sure I have examples for all those questions, but certainly, over-reporting can be a problem. It is sort of the boy who cried wolf. If you get notices over and over that actually don't pertain to you, you may start to ignore them, but worse, you may actually start making changes to your passwords and closing and opening bank accounts unnecessarily, wasting your own energy. So the different State regimes can cause over-reporting, which can harm consumers, and it also certainly impacts businesses in being able to comply with those laws.

Mr. OLSON. It looks like the professor wants to make comments. Ma'am, you are up.

Ms. MATWYSHYN. I wanted to play up on that point. The two complaints—I shouldn't say complaints. The two comments that I have heard repeatedly from businesses in their compliance efforts, first, that the regulatory end of this complicated. Different regulators are required to receive filings in different States so simplifying the regulatory complexity would be something they would want.

The second point that they repeatedly mention to me is the definition of what constitutes information that triggers reporting, and

they would be happy with a broader definition of the information that triggers information as long as it is a bright line, it is clear to them. And so many companies, especially the most sophisticated technology companies, are now erring on the side of reporting because it is simpler, and they don't view it necessarily as a bad thing, they just want simplification and a single regulatory point of contact.

Mr. OLSON. And I would assume when they go public that they have had some data breach, that affects their business because consumers look at a company that has had a data breach, maybe is having some faults, which is not true, but the bottom line, in the market they get spooked and move their products elsewhere. One more comment, ma'am. I am out of time.

Ms. MATWYSHYN. If I can just follow up, the other benefit that a centralized point provides is the ability for companies engaging in highest security practices to announce that. So even if they suffer a data breach from a zero day vulnerability, for example, if they are using the highest end software possible, then enforcement agencies are going to say oh, they tried really hard, this is a good company doing the right thing. But if it is someone who hasn't updated their systems in 6 years and that is why they had a data breach, that is a completely different ball of wax.

Mr. OLSON. I am out of time. I thank the witnesses, and come to Texas.

I yield back.

Mr. TERRY. No.

Mr. Johnson, you are recognized.

Mr. JOHNSON. Also no, Mr. Chairman.

I would like to thank the panel for being here today. I spent about 30 years of my professional career before I came to Congress in the information technology field in the Department of Defense, worked as the director of the CIO staff for special operations command, so I certainly understand the complexities of data security and how easy it is for those who are determined to get into it.

So with that as a backdrop, do we have any empirical data to answer the question about how quickly we should notify consumers? I mean, do we have any data that tells us after several hundred thousand identities are breached, do we know how long before the bad guys start using that information? Anybody on the panel? Mr. Greene?

Mr. GREENE. Unfortunately, there is no answer. There are thriving black markets in personal information, whether it is a Social Security number, et cetera, or simply credit card numbers, and it can be a game of roulette whether your card is bought before it goes stale or not, so we don't know how fast. It really depends on how they are going to use their information. Slightly off point, but there is empirical evidence. The Ponemon study from last year found—it was looking at the impacts, and one of the drivers of increased costs was notification too early. What they found is, companies that rushed to notify often notified a significant number of people who once they did their full forensic work had not actually had their personal information made public, yet the companies notified them. The individuals, many of them, went to the trouble of changing passwords, etc. The company had to pay for monitoring

and other services. So we do know—and again, not discounting the need to notify quickly but doing it too quickly can drive up costs, both for the individuals and the companies.

Mr. JOHNSON. Speaking of quickly or not quick enough, do you think that breaches are over- or under-notified today? Again for the entire panel. Does anybody have a thought? Yes, ma'am.

Ms. MATWYSHYN. I would say they are dramatically under-notified. Frequently, they are never discovered, and that is partially because companies unfortunately don't always have state-of-the-art security in the place. Also in the public sector, we have the same challenges with security. So I would assume there are two breaches for every one that is reported.

Mr. JOHNSON. Given that there is a plethora of State regulations that require this, do you think an overarching federal standard lessons the risk of under- or over-notification?

Ms. MATWYSHYN. I think it is heading in the right direction. I think we are improving. We are all becoming more educated about these issues. Companies are becoming more sensitive. There is dramatic improvement in the last decade, and particularly in industries such as financial services, they are improving, and there is a learning curve happening, so we are heading in a good direction, and I think federal harmonized legislation is a step in that direction.

Mr. JOHNSON. Mr. Richards, you noted that the FTC has been relatively active in bringing cases against companies for failure to maintain or disclose their security practices. If the FTC has this existing authority, do we need to address data security in more federal legislation?

Mr. RICHARDS. Congressman, in reference to your last point, I believe strong federal preemptive data breach notification law that is broad in scope would cut down on over-notification certainly. We believe that the FTC does have a lot of jurisdiction within its existing authority but we believe given the patchwork quilt of 48 different State laws that a broad federal preemptive law would be very helpful to our businesses.

Mr. JOHNSON. Well, I think I know the answer to this next question, Mr. Richards, but can data security and data breach notification be addressed separately or are they hand in hand?

Mr. RICHARDS. Well, I think they can be. Well, I would suggest addressing them separately, first data breach notification, getting some consensus on the committee. I think certainly the conversation around data security is important. I think there should be some focus on what we have been talking about in terms of a safe harbor, how do you incentivize companies or give companies some type of guidance on how they render the data useless so if it is hacked or stolen, you have taken the measures and you shouldn't have to report. So I think certainly as a balance, a lot of the focus has been on what happens post breach but I certainly think there are some measures they can take pre-breach.

Mr. JOHNSON. Great. I think I am last, Mr. Chairman. If you would indulge for one more?

Mr. Greene, you stated that there were 93 million identities exposed in 2012. Does this mean people, their names, their user

names or their Social Security numbers? What does identity mean in that 93 million number?

Mr. GREENE. By the way we counted, it was name in connection with Social Security number, address—one of the following: Social Security number, address, date of birth, or credit card information. Essentially, information that put together would allow financial fraud or identity theft.

Mr. JOHNSON. All right. Thank you, Mr. Chairman. I yield back.

Mr. TERRY. Well done, everybody, so that concludes the questioning period, which means that we are finished except for a little bit of work here.

I ask unanimous consent to include the following statements in the record: one, statement of the Electronic Transaction Association dated July 18, 2013; two, a letter from the Credit Union National Association, CUNA, dated July 17, 2013; a letter from McDonald Hopkins LLC dated July 18, 2013; number four, National Retail Federation statement dated July 18, 2013. These have all been approved by the minority staff. Hearing no objections then, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. TERRY. No documents to be submitted on your side. Now all of our business is done, and I want to thank all of you. It has been very insight. It was very stimulating, and we greatly appreciate your time and your testimony, which is your talent, and thank you, and we are adjourned.

[Whereupon, at 1:24 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. FRED UPTON

Those of us who have been in Congress more than a term or two know the issue of informing consumers in the event of a data breach has been around for a number of years.

The importance of protecting our personal information grew as the crimes of identity theft and financial fraud became more pervasive in our digital world. It's a fact of life almost every citizen has some digital footprint or profile—whether from the state and county records, school records, or transaction with businesses.

As we enjoy the wonderful new conveniences and efficiencies provided by the technology, the downside is that it also facilitates the ability of criminals to act with equal efficiency to commit identity theft or other crimes that can potentially injure far more consumers' credit and finances. No longer is a criminal confined by what he can gather from a few paper based records taken from a mailbox or file cabinet. Rather, the most sophisticated of today's cybercriminals can attempt to hack into digital databases and gain access to the data on millions of individuals.

Data breaches were a somewhat novel issue 8 years ago when we first learned of it. Our constituents were being notified of a breach of their information for the first time under a handful of state notification laws. The landscape has evolved and notifications have become more common, as have breaches and state notification laws: we now have laws in 48 states and territories, including every state represented on this dais except for one—many of which have slight differences—as well as a separate federal notification law addressing breached health information. Entities holding our personal information have also evolved, incorporating security as an essential part of their operation. Experience has demonstrated the harm to their customers and the entity's reputation are reason enough to encourage those who hold our information to take reasonable steps to protect it.

Yet breaches, identity theft, and financial fraud continue and we must consider whether the current notification regime is appropriate. I believe timely notification is an important aspect of helping consumers protect themselves following a breach of their information—and I question whether having to examine 48 different laws before notifying one's customers is helpful to this goal. If the breach was intentional or if the data falls into the hands of criminals with malicious goals, the consumer

should be aware to take preventative steps to protect or monitor their accounts more closely. Dealing with identity theft or account fraud can be an expensive and time consuming ordeal for a victim.

I think the title of the hearing is an appropriate question to ask: "Is Federal Legislation Needed to Protect Consumers?" Certainly no one would propose 48 variants of the same law—each with their own compliance requirements—as an efficient way to address any problem. Can a Federal notification law replace the state laws in a way that maintains the protections afforded by the states and minimizes consumer confusion? I think the potential benefits to both consumers and businesses from a single standard make this an issue worthy of our time. I welcome our witnesses and look forward to discussing their perspectives.

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
1.800.695.5509
202.828.2635
202.828.2639

Statement of the Electronic Transactions Association

United States House of Representatives
Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade Hearing:
"Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?"
Thursday, July 18, 2013

In anticipation of the Commerce, Manufacturing, and Trade Subcommittee's July 18 hearing, the Electronic Transactions Association ("ETA") -- an international trade association representing companies that offer electronic transaction processing products and services – submits the following statement for the hearing record.[1] ETA's comments are intended to assist in the Subcommittee's examination of the necessity of federal data breach legislation.

The ETA believes that a uniform national standard for data breach notification will best address the rights of consumers to be notified of a breach when the security of their Personally Identifiable Information ("PII") is truly at risk. Any such national standard should attempt to minimize the compliance risk to businesses. Today, payment processors are forced to comply with an ever-changing array of 47 different state laws on breach notification, a significant challenge to the industry's goal of protecting all consumers against data breaches with uniform national practices.

ETA recommends that any federal breach notification legislation incorporate the following:

A Clear Notification Triggering Mechanism

A clear notification triggering mechanism is essential to facilitating compliance. Legislation should establish a standard for data breach notification that requires notice only when it is determined that there is an actual risk of fraudulent use of compromised PII.

Unambiguous Preemption of State Law

In order to provide consumers with a consistent level of protection, any federal data breach legislation must establish a uniform national standard for data breach notification. Ambiguous state preemption provisions will place businesses in the unenviable position of having to navigate a variety of state laws (at present, 47 different state laws). This is precisely the predicament any legislative proposal should aim to prevent.

[1] ETA represents more than 500 companies that provide payment processing services, including card networks, financial institutions, processors, manufacturers, independent sales organizations, and technology companies.

A Succinct Definition of Personally Identifiable Information

Any definition of PII should be limited to an individual's full name, biometric data, email address, street address, telephone number, full Social Security number and/or personal financial information. The inclusion of various combinations of data elements, especially marginal identifiers (*e.g.*, mother's maiden name, passport number, etc.), will create a compliance standard that is nearly impossible for businesses to adhere to.

Reasonable Notification Requirements

A number of parties in the payment chain will not have access to the contact information necessary to directly notify persons whose PII has been compromised. Federal data breach legislation should allow reasonable time for the party that suffered the data compromise to fulfill any notification obligations by identifying and notifying the industry member in possession of the essential contact information to deliver any required notices.

Recognition of the Existing Legal Framework

Federal data breach legislation should provide a compliance "safe harbor" for entities subject to the Gramm-Leach-Bliley Act or the Fair Credit Reporting Act without making additional parties subject to such banking laws and regulations. This will prevent duplication with existing law that will result in additional, unnecessary, and unproductive regulation.

Acknowledgement of Industry Self-Regulatory Efforts

Federal data breach legislation must provide a "safety net" for effective industry governance related to protection of transactor data. For example, efforts by payment networks (*e.g.*, American Express, Discover, MasterCard, Visa) to establish the Payment Card Industry-Data Security Standards ("PCI-DSS") represent effective security controls by the parties in the best position to ensure that the standards evolve as technology and risk profiles develop and change over time. Any additional regulation should build upon and reflect existing efforts.

* * * * * * *

The payments professionals comprising the ETA's membership take seriously their obligation to protect the confidentiality and security of their customers' credit, debit, and other non-public financial account information. The current patchwork of state laws provides inconsistent protection for consumers and the varying standards established by these laws have created serious compliance challenges for businesses of all types.

As the Subcommittee's examination of federal data breach legislation proceeds, the ETA looks forward to sharing additional information regarding the impact of federal data breach legislation on the payments industry.

CUNA
Credit Union National Association
cuna.org
BILL CHENEY
President & CEO

601 Pennsylvania Ave., NW | South Building, Suite 600 | Washington, DC 20004-2601 | PHONE: 202-508-6745 | FAX: 202-638-3389

July 17, 2013

The Honorable Lee Terry, Chairman
Subcommittee on Commerce, Manufacturing and Trade
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Terry:

On behalf of the Credit Union National Association (CUNA), I am writing about today's hearing entitled "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?" CUNA is the largest credit union advocacy organization in the United States, representing America's state and federally chartered credit unions and their 96 million members. We are pleased to offer comments for the hearing record on this very important topic.

The chain of data security is only as strong as its weakest link. A data breach can occur anywhere along the payments transaction, from the merchant, to the merchant bank, the issuing card bank, and ultimately the financial institutions. As we describe below, credit unions are subject to very high data security standards under the Gramm-Leach Bliley Act of 1999 (GLBA).[1] However, merchants are not required to follow these standards, and until they are held to the same standard, consumers will remain vulnerable to a system that does not protect their information.

We encourage Congress to consider legislation that holds merchants to the same standards as financial institutions when they handle financial transactions, and that permits financial institutions to disclose the source of the data breach and seek reimbursement from the merchant for the cost of the breach.

Merchant Data Breaches

Merchants benefit greatly from the electronic payments system. The largest benefit to the merchant is the elimination of risk they would otherwise have to assume if the transaction were paid with cash (theft risk, handling and security costs) or a check (bounce risk, which includes non-payment and collection expenses). Merchants also benefit from streamlined accounting, reduced credit risk, faster check-out and increased purchase amounts compared to checks or cash.[2]

[1] P.L. 106-102, Title V (November 12, 1999).
[2] Adam J. Levitin. —Interchange Regulation: Implications for Credit Unions. Filene Research Institute. 6

CREDIT UNIONS

PO Box 431 | Madison, WI 53701-0431 | 5710 Mineral Point Road | Madison, WI 53705-4454 | PHONE: 608-231-4000

With the electronic payment system, card issuers, such as credit unions, assume all of the risk and guarantees the merchant will receive payment. In the process, the consumer receives a very important service: an efficient, convenient, seamless, and universally-accepted transaction. That very consumer service redounds to the benefit of merchants. The easier it is for a consumer to access his or her funds at the point of sale, the more likely he or she is to spend them on the goods or services the merchant is offering. There is tremendous benefit and value attached to the debit card, as evidenced by the significant increase in its acceptance by merchants and its use by consumers over the last decade.

The question is: What happens when something goes wrong? Unfortunately, merchant data breaches happen, and experience tells us, it is the card issuers who take the loss and take steps to protect the consumers. In the event of a merchant data breach there are no federal requirements for merchants to notify consumers of that breach. The onus of notification to the consumer lies on the financial institution that issued the payment card. However, financial institutions cannot specify which merchant was responsible for the breach and also bears the costs of issuing new payment cards, and making any loss to the consumer's account whole. The merchant bears no financial responsibility in the case of a data breach.

Merchants are not subject to federal data security requirements, nor are they financially liable for damages. In some cases, merchants do not even face reputational risk as a result of a breach because they are not required, under federal law, to disclose a breach. The financial institutions of consumers affected by the breach in most cases do not know the source of the breach, and when the source is known, are not permitted to identify the merchant responsible. While there are industry standards, merchants are not required by law to follow these standards.[3]

Until there are consequences to these bad actions, voluntary standards will not be sufficient to protect consumers. It is common sense that if merchants receive benefits from debit cards payments that they should be subject to the same high data security standards as financial institutions. To protect consumers, Congress should require merchants to be regulated to at least the same extent that financial institutions are when it comes to data security. In the event of a merchant data breach, Congress should allow financial institutions to name the source of the merchant data breach and require the merchant responsible for the breach to be financially liable for the cost of the breach of the affected consumers and financial institutions.

Data Security Requirements for Credit Unions

The National Credit Union Administration (NCUA), implements data security standards for credit unions, as does the Federal Financial Institutions Examination Council (FFIEC), of which NCUA is a member.[4]

---

[3] In 2004, the card brands agreed to a common worldwide standard for the protection of cardholder data, as defined by the Payment Card Industry Security Stands Council. Payment Card Industry Data Security Standards (PCI DSS) applies to all organization that hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands.

[4] The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. Its membership includes leadership from the Federal Reserve Board, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee. The Office of Thrift Supervision, a past member, was eliminated in July 2011, and many of its functions transferred to the Office of the Comptroller of the Currency.

Credit unions are subject to data security requirements as required by §501(b) of the GLBA and Part 748 of the NCUA's regulations. Specifically, under §501(b) of the GLBA, Congress required NCUA and other federal financial regulators to establish standards to ensure financial institutions protect the security and confidentiality of the nonpublic personal information of their members or customers.

Part 748 of NCUA's regulations requires credit unions to establish a comprehensive data security program addressing the safeguards for customer records and information. These safeguards are intended to insure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against any unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer. In addition, Part 748 also requires credit unions to develop and implement "risk-based" response programs to address instances of unauthorized access to member information.

Data security requirements under the GLBA and NCUA's regulations are subject to the supervision and enforcement of NCUA for federal credit unions or the state supervisory agencies for federally-insured state-chartered credit unions. Additionally, the Federal Trade Commission has enforcement authority for compliance with these requirements for state-chartered credit unions.

Federal banking agencies have developed and published additional information security requirements which cover specific threats and mitigation of identified risks. The FFIEC has issued specialized IT handbooks that outline cyber security requirements for all depository institutions within the banking and finance sector. The FFIEC IT Handbooks are actually comprised of 11 separate booklets, and are very similar to the current cyber security guidance that pertains to federal agencies. The IT Handbook addresses various topics, including (1) audit, (2) business continuity planning, (3) development and acquisition, (4) electronic banking, (5) information security, (6) management, (7) operations, (8) outsourcing technology services, (9) retail payment systems, (10) supervision of technology service providers, and (11) wholesale payment systems. Credit unions are required to adhere to this FFIEC guidance and these requirements are incorporated into NCUA's examination practices for credit unions, as further detailed below.

The methodologies that federal banking regulators including the FFIEC and NCUA use to provide oversight and supervision vary, but include periodic examinations, self-reporting, and other administrative and legal supervisory actions to enforce compliance.

NCUA has also issued regulations that outline data security and anti-identity-theft requirements, along with publishing agency Letters to Credit Unions, Regulatory Alerts, Legal Opinion Letters and final regulation Part 748 addressing credit union security programs. NCUA's examiners use Automated Integrated Regulatory Examination Software (AIRES) consisting of multiple information technology examination questionnaires to assist with reviewing a credit union's information systems and technology. These AIRES examination questionnaires incorporate all

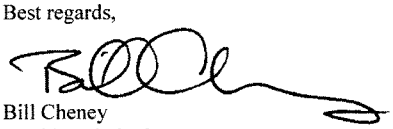
of the supervisory requirements contained within the FFIEC's IT Handbooks previously discussed. Each of these additional regulatory measures and guidance documents have been developed over the last several years in response to data security and other cyber security and consumer protection laws, some of which include the GLBA and the Fair Credit Reporting Act.

Additionally, Part 716 of NCUA Rules and Regulations governs credit unions' use of customer and member non-public personal information, in accordance with Title V, Subtitle A of GLBA, which contains various requirements including prohibitions on sharing of account numbers, a requirement that all credit unions provide privacy notices to members and customers, and when applicable, credit unions must also provide a conspicuous notice that explains the right of the person whose non-public personal information is going to be shared with certain nonaffiliated parties to "opt out," and credit unions must provide a reasonable means by which and a reasonable time in which the person may exercise the opt-out right. Other provisions of Part 716 include a prohibition on sharing account numbers with third parties for marketing purposes, and limitations on the re-disclosure and reuse of information shared with nonaffiliated third parties.

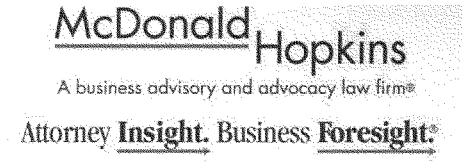
Conclusion

Data security is a critical issue, and it is clear that there are areas where Congress needs to consider legislation. To protect consumers, Congress should require merchants to meet the same high standards for data protection to which financial institutions are subject. In addition, Congress should permit financial institutions to disclose the source of data breaches affecting their members or customers, and merchants should be required to reimburse consumers and financial institutions for the costs associated with data breaches.
On behalf of America's credit unions and their 96 million members, thank you again for holding this hearing. We appreciate your leadership on this issue.

Best regards,



Bill Cheney
President & CEO



McDonald Hopkins LLC

for the record

House Energy and Commerce Committee

Subcommittee on Commerce, Manufacturing and Trade

Examining State Breach Notification Laws and Potential Federal Preemption

July 18, 2013

McDonald Hopkins LLC thanks Chairman Terry and Ranking Member Schakowsky for holding this important hearing on the potential federal preemption of state breach notification laws.

McDonald Hopkins' national Data Privacy and Cybersecurity practice, led by attorneys James J. Giszczak and Dominic A. Paluzzi, counsel clients in numerous industries, including, education, healthcare, hospitality, retail, automotive, accounting, finance, information technology, staffing services, manufacturing, utilities, professional employer organizations, fleet services, franchising, drug and pharmacy, and insurance. The Data Privacy and Cybersecurity attorneys at McDonald Hopkins regularly advise clients regarding data privacy and network security measures, drafting of written information security programs and incident response plans, and training of employees with access and exposure to sensitive personal data. The McDonald Hopkins team specializes in breach coaching through the myriad of state, federal and international breach notification laws. Our attorneys also serve as panel counsel for the major carriers of privacy and cyber insurance coverage, acting as a resource for insureds, providing all cybersecurity related services-from proactive measures to breach coaching to litigation defense, including both single plaintiff and class actions.

According to the Privacy Rights Clearinghouse, more than 608,278,176 records have been reported compromised since 2005. Of course, many more have gone unreported, so this figure is probably three to five times higher. Eighty five percent of the data privacy incidents are not considered difficult, according to a recent Verizon study. Although the foreign hackings make the headlines, most data privacy incidents arise out of simply lost devices (laptops, USBs and smart phones). What is difficult for every organization, however, is attempting to comply with each of the 46 different state breach

notification laws, as for most, they are confusing, therefore leading to under-reporting, failing to act or non-compliant notifications.

Before analyzing the differences between the state breach notification laws, which there are many, it is important to consider the various federal privacy and security laws, which can also be confusing to organizations, as they too play a significant role in the notification process. A few of the federal privacy statutes that often must be considered include: Health Insurance Portability & Accountability Act of '96 (HIPAA), Health Information Technology for Economic & Clinical Health Act (HITECH), Gramm-Leach-Bliley Act (GLBA), and the Federal Trade Commission (FTC) Red Flags Rule. There are also burdensome private regulations that organizations are required to comply with, such as the Payment Card Industry Data Security Standards (PCI DSS), for those handling bank cards. We are often told by our clients, "I'm just trying to run my business; all of this is very confusing and a huge distraction." However, there are very good reasons that these various statutes are in place. Most critically, less than 40% of businesses actually have a plan in place to respond to a data privacy incident. And those that do have plans in place typically have insufficient and inadequate plans that barely scratch the surface. Without these statutes, organizations would be driving down the highway at their own pace, from 20mph to 200 mph. There would be no parameters to provide even a minimal level of order or safety for the general public.

All states, with the exception of Alabama, Kentucky, New Mexico and South Dakota have a unique breach notification law. In fact, many experts argue that Texas' recently revised statute even covers the four states that do not currently have a breach notification law. Organizations in those four states, as well as the other forty five, often ask how and why Texas lawmakers could possibly impact their businesses. The key to understanding these laws is that the residency of the affected individual governs which state breach notification law must be followed. It is irrelevant where the company is headquartered or where the device was stolen. Thus, in a majority of the standard data privacy incidents, it is typical that several state notification laws, and possibly one or more federal statutes, must be complied with.

The state breach notification laws currently in place in 46 jurisdictions differ, in part, as follows:

(1) **How Personal Information (PI) is defined.** Most states include name, Social Security number, Driver's License number, and financial/credit card account information as PI. Some states include medical information in their definition of PI. Alaska, for instance, includes ATM PINs in the definition of PI. North Carolina includes biometric data and finger prints.

(2) **What constitutes a "data breach".** There are approximately 12 variations of thresholds that trigger notification of a data breach. Examples of the standards are as follows: "reasonable likelihood of harm to an individual"; "when the incident could result in identity theft" "whether PI is subject to

further unauthorized disclosure"; "when misuse of PI has occurred"; or "when the incident is likely to cause loss or injury or economic loss or financial harm"

(3) **Whether an incident involves computerized or paper records**. Some state statutes are only triggered if the loss of personal information was in a computerized format. Others include hardcopy incidents as well. This seems particularly odd as the information could be misused in either media.

(4) **When to give notice**. States vary on the timing that affected individuals must be notified; from 5 days, 30 days, and 45 days or "without unreasonable delay".

(5) **Additional parties to receive notice**. Many states require the state's attorney general to receive notice of a breach. Other states, such as New Jersey, want their State Police notified. Massachusetts requires its Office of Consumer Affairs be notified. New York requires the Consumer Protection Board & Office of Cyber Security to receive notice of the breach.

(6) **Contents of the Notice**. Some states require specific-incident facts be included in the notice letter, such as the date of the incident, date of discovery, the type of PI at risk, and toll-free numbers to consumer reporting agencies. Some states, such as Maryland and North Carolina, require that the state attorney general's contact information be included. The Massachusetts' statute, on the other hand, does not allow the notifying organization to include incident-specific facts in the letter to affected individuals. Thus, one size does not fit all and organizations cannot use one template letter for all affected individuals. If they did, their notice letters could be a further violation of the applicable statutes.

As if the requirements in the statutes are not burdensome enough, many of the regulations include significant penalties for failing to comply with the data privacy statutes. A few of the legal penalties include: up to $750,000 in penalties to the company for failure to notify affected individuals, $10,000 per violation for officers/directors personally, up to $1,500,000 for repeat HIPAA violations under the Final Rule, officers/directors can serve up to five years in prison, banks can lose FDIC insurance, and state privacy statutes provide for private civil actions for instances of non-compliance, including punitive damages and attorneys' fees.

Based on the information we have discussed, McDonald Hopkins has two primary recommendations.

(1) **The need for uniformity**. We urge the subcommittee, however, that if it considers a federal breach notification statute to preempt the 46 state statutes, careful analysis of each of the 46 statutes must be conducted. The federal law would ideally implement the best provisions from each of the current state statutes in an effort to provide the citizens of this great Country the most

protection possible, without being over burdensome on the organizations that are the engine of our economy.

(2) **The need for preventive policies**. We strongly encourage the subcommittee to examine information security laws which would require organizations that have access to, use or disclose personal information, to implement certain strict preventative policies. For example, proactive measures can include drafting of a Written Information Security Program and Incident Response Plan, conducting employee training, and audits of internal policies, as well as data privacy measures utilized by a third-party vendor. One-third of all breaches are the result of a vendor incident and not the company itself that significantly invested in the security of its system. A federal law should require organizations to implement proactive measures and policies to help minimize the risk of a data breach requiring notification.

Statement of the

National Retail Federation

and

Shop.org

submitted to the

United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing and Trade

for its hearing on

"Reporting Data Breaches:
Is Federal Legislation Needed to Protect Consumers?"

held on

Thursday, July 18, 2013

David French
Senior Vice President
Government Relations

On behalf of:

National Retail Federation
325 7th Street, N.W., Suite 1100
Washington, D.C. 20004
(202) 783 –7971
www.nrf.com

Chairman Terry, Ranking Member Schakowsky and members of the Subcommittee on Commerce, Manufacturing and Trade, on behalf of the National Retail Federation and its division, Shop.org, I appreciate the opportunity to submit this written statement to the Subcommittee in connection with its hearing entitled "Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?" held on July 18, 2013.

As the world's largest retail trade association and the voice of retail worldwide, NRF represents retailers of all types and sizes, including chain restaurants and industry partners, from the United States and more than 45 countries abroad. Retailers operate more than 3.6 million U.S. establishments that support one in four U.S. jobs – 42 million working Americans. Contributing $2.5 trillion to annual GDP, retail is a daily barometer for the nation's economy. Retailers create opportunities for life-long careers, strengthen communities at home and abroad, and play a leading role in driving innovation. Shop.org, a division of NRF, is the world's leading membership community for digital retail. Founded in 1996, Shop.org's 600 members include the 10 largest online retailers in the U.S. and more than 60 percent of the *Internet Retailer* Top 100 E-Retailers. Data and data privacy are matters considered by all our members.

Comments

Information is a vital component of the retail industry, and a catalyst for its growth. Trends and revolutions in retailing, such as the rise of e-commerce, are fueled by the sharing of information between merchants and their customers. Among other things, the data collected by retailers ensures the right merchandise is stocked on shelves, customers are offered the best sales and promotions to get them in the door, and stores are opened in locations where demand is the highest.

Retailing is a very competitive industry. Most retailers have direct, first-party relationships with customers and want to maintain those relationships. Retailers compete to keep customers. To do so we must provide real value and earn our customers' trust. An important part of that trust is ensuring that customers know "we're in this together." Data protection and privacy are a part of that equation: the more critical the information, the greater the care.

We agree with the Subcommittee that data security considerations should be taken seriously by all businesses – from securing human resources information to protecting databases that hold sensitive information, such as customer financial information held by banks and other financial institutions. Increased security often requires increased resources. The data security protections employed should be commensurate with the sensitivity of the data. The level of security deployed to protect one's banking details, for example, should naturally be higher than the level invested in cordoning off an individual's shoe size.

We believe that when the confidentiality of sensitive data has been compromised due to a criminal hacking or otherwise, the first obligation of a responsible business is to arrest the loss of data, and then to contact customers if there is a likelihood of a significant risk of harm. Individuals may take steps to contain potential consequential losses while the business take steps to further contain the breach, secure information, and restore the integrity of systems. After extended consideration of this need, and the various alternatives, most states have adopted laws to accomplish these goals. As a result, during the past decade retailers across the nation have remediated breaches of security in this fashion and provided notice to affected customers in

compliance with the laws of 46 states and four other federal jurisdictions, including the District of Columbia, that govern the reporting of data security breaches.

While we would support federal legislation that creates uniform national data security standards along the considered lines the states have adopted, some of the proposed breach notification provisions in federal data security and cybersecurity bills introduced in Congress over the past several years have been highly problematic. We would not object to a federal bill that achieves its stated purpose of creating a national standard that preempts inconsistent state breach notification rules, provided the federal standards are similar in nature and design to the most common of the existing state laws. Such a federal law would simplify the response of those companies who operate in multiple states; and it would ensure that consumers could come to understand and rely upon a uniform notification system, regardless of where a breach might occur. However, we would strongly object to a federal bill that does not preempt the existing inconsistent bills – thus effectively creating a 47th 'state law' – or that purports to expand the federal regulatory regime beyond the confines of the existing state framework to include new and novel provisions or impose new data regulations unrelated to breach notification.

For example, from the Subcommittee's previous work, we understand there is an interest by some in having customer notification tied to breaches of non-sensitive data, such as publicly available e-mail addresses and the like. Most states, however, only require notification of sensitive personal information of the kind that could be used to commit identity theft or other financial crimes against an individual. Furthermore, we would bring to the Subcommittee's attention that many entities hold much more sensitive personal data of their customers than a typical retailer, such as the kind of customer financial account and investment information held by financial institutions. Those entities have traditionally been excluded from this Subcommittee's legislation due to jurisdictional considerations, even when the resulting data security legislation, if enacted, would create a federal statutory regime where less sensitive data is subject to greater regulation and penalties than the more sensitive personal data that could actually lead to identity theft if breached. To avoid this type of upside-down, unintended consequence, NRF would urge the Subcommittee to consider and apply in any legislative drafting on this issue the data security principle long-endorsed by the Federal Trade Commission (FTC), the Organisation for Economic Co-operation and Development (OECD) and other governmental entities that have focused on these issues – simply, that information security should be proportionate to the type and sensitivity of the data.

There is an old saying that "the customer is always right": retailers must meet customers' constantly evolving expectations. If retailers do not meet their customers' expectations or, worse, violate that trust, customers will simply shop elsewhere. Considering the limitless number of shopping choices presented to American consumers every day, particularly online and on their mobile devices, there's a new saying in retail that is particularly appropriate in this context: "Competition is only one click away."

Given the general alignment between retailers' and their customers' interests in terms of satisfying their needs and allaying their concerns, and the relative lack of sensitivity of most shared data, honoring consumers' privacy and securing their data is a goal we can regularly reach. For this reason, retail customers are very likely to have their privacy and data security expectations met, and customers will continue to maintain significant control over the business relationship. The FTC recognized as much in its December 2010 staff report on a proposed U.S.

privacy framework (the "FTC Privacy Report"), noting that it had less concerns about these types of consumer information practices than others.[1]

Conclusion

Retailers take the privacy and security of their customers' information seriously, and are motivated both by the desire to follow good business practices as well as a basic concern of maintaining their customers' satisfaction. They do not want to lose the loyalty of their customers as the result of a sophisticated criminal hacking of retailers' protected systems. We appreciate the Subcommittee's focus on data security legislation, and we believe that hearings help clarify many of the issues surrounding the protection of customer information already in place as best business practices. As it has often been said, "sunlight is the best disinfectant," and an ongoing dialogue between the Subcommittee and the business community over data security issues is very useful. In particular, the Subcommittee's ongoing interest in these issues encourages businesses to consider more carefully any changes in data collection, use or protection that may make consumers feel uncomfortable about the safety and security of customer information.

That being said, we would encourage the Subcommittee to carefully evaluate the need for federal data security breach legislation given the existing and effective state framework with which retailers victimized by breaches have complied in notifying their customers. If the Subcommittee decides to move forward with legislation, we would respectfully suggest the Subcommittee create a single, national standard with provisions similar to, and preemptive of, existing state security breach laws, and not extend the focused framework already employed by the states that has served both consumers and businesses well over the past decade.

NRF thanks the Committee for their examination of data security breach notification and is happy to work with Members of the Committee as it considers such legislation this Congress.

[1] *See* Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change," December 1, 2010 (hereinafter, "FTC Privacy Report").